

Congress of the United States
Washington, DC 20515

February 8, 2016

Mr. Norman Dong
Public Building Service Commissioner
General Services Administration
1800 F Street NW
Washington, DC

Dear Commissioner Dong,

Since passage of the Southeast Federal Center Public-Private Development Act of 2000 (P.L. 106-407), the General Services Administration (GSA) has worked with its master developer partner, Forest City Washington, to realize the stated purpose of the statute we got Congress to pass in 2000 to bring the Southeast Federal Center to productive use for the benefit of taxpayers. Progress is well underway toward meeting the goal of producing 5.5 million square feet of commercial development on the 42-acre property, which provides revenue from this site to the federal government for the first time.

However, an unanticipated hurdle has arisen that should have been clarified by now, considering the ongoing development agreement between GSA and Forest City Washington. That agreement provides that if any office buildings are built (totaling up to 1.8 million square feet of the 5.5 million square feet approved for development), they will be on ground leases granted by GSA to Forest City Washington. Forest City Washington is required to pay ground rent to GSA when office buildings are erected on the site whether or not leased by GSA.

Our offices seek clarification from GSA in light of the position that Forest City Washington has taken that ground rent payments made to GSA should be considered against any space rent Forest City Washington proposes in competitive lease procurements when deciding which bid offers the lowest cost lease to the federal government. For example, Forest City Washington argues that \$45 million in rental payments would have been paid to GSA over the term of a major GSA lease had the Forest City Washington proposal been selected. Because of GSA's concerns about fairness to other competitors, that sum went unrecognized by GSA in evaluating all the lease proposals in the procurement. This issue is likely to arise in procurements elsewhere and has not been affirmatively answered explicitly as a matter of GSA policy. We are requesting that GSA explicitly answer the question posed by this dilemma and

the reasons for the GSA position. We have been asked, for example, if a developer required to pay ground rent to GSA offered \$501 million while the winning competitor offers \$500 million, would GSA, which is guaranteed the start of payments totaling \$45 million returned to itself without delay (and thus the taxpayer), consider this amount over the course of the lease in the lease competition.

Would the federal government have also accelerated the timeline for its reversionary interest in the property activated at the end of the lease? Once the improved property reverts back to the federal government, any rental payments being paid by a federal agency go into the Federal Buildings Fund instead of to Forest City Washington. The Federal Buildings Fund, of course, is used to fund new construction and repairs of existing GSA controlled facilities. Would the eventual addition of the office buildings constructed by Forest City be a significant benefit to taxpayers?

We make these inquiries considering that GSA has previously acknowledged similar economic advantages in competitions for leased space. For instance, GSA consistently recognizes that existing capital investment in leased premises offers vested incumbent lessors an economic advantage unavailable to any other competitors because of the potential avoidance of the costs of moving a federal agency and replacing furniture, fixtures and equipment when considering new space.

As you can see, a dilemma results for all concerned. Does Forest City Washington get a competitive advantage in some cases if its ground rent encourages GSA to select Forest City Washington for a parcel? On the other hand, are taxpayers at a disadvantage when another landlord is selected but taxpayers get no ground rent or ground rent is delayed while Forest City Washington waits for another tenant as a result of the lease award? The Southeast Public Private Redevelopment Act did not oblige GSA to take space in any building constructed on this site. The Act appears to be less clear, however, about how that ground rent is considered when GSA is leasing for the government. In light GSA's current policies to capture added value for the government, what does GSA believe the intent of the Act to be? We would appreciate your position on this matter. Please advise us of your findings within 60 days.

Sincerely,



Lou Barletta
Chairman, Subcommittee on Economic
Development, Public Buildings, and
Emergency Management



Eleanor Holmes Norton
Senior Member, Subcommittee on
Economic Development, Public Buildings,
and Emergency Management



GSA Public Buildings Service

April 8, 2016

The Honorable Lou Barletta
Chairman, Subcommittee on Economic
Development, Public Buildings, and
Emergency Management
House of Representatives
Washington, DC 20515

The Honorable Eleanor Holmes Norton
Senior Member, Subcommittee on
Economic Development, Public Buildings,
and Emergency Management
House of Representatives
Washington, DC 20515

Dear Chairman Barletta and Congresswoman Norton:

Thank you for your letter dated February 8, 2016, regarding the U.S. General Services Administration's (GSA) development agreement with Forest City Washington (FCW), entered into pursuant to the Southeast Federal Center Public-Private Development Act of 2000, P.L. 106-407 (the "Act"). GSA is open to discussing with FCW any specific proposals and respective cost benefit analyses it might have regarding how the development agreement may be improved for the benefit of taxpayers. GSA would also encourage FCW to compete in any leasing procurements and to offer competitive pricing.

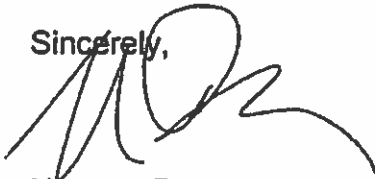
The exclusive development rights conferred on FCW through the development agreement already provide FCW with a competitive advantage in the context of competitive GSA space actions. Given the number of development projects achieved since 2005 in the Southeast sector of the District, the ground lease rental rates established in the development agreement are presently below market rates such that FCW likely already enjoys an advantage as a developer with respect to land costs. GSA believes that FCW could make competitive offers in terms of price, either to the Government or the private sector. Should FCW compete in and win a GSA lease procurement FCW and GSA then could discuss offsetting ground lease payments against space.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
Telephone: (202) 501-1100
Fax: (202) 501-2300
www.gsa.gov

You have asked, specifically, how GSA would treat, for evaluation purposes, ground rent payments payable to GSA from FCW in a competitive lease procurement where FCW was a participant. The Act does permit in-kind consideration, including the provision of office space. However, the negotiated development agreement between GSA and FCW makes no provision for FCW being able to offset ground rent payable to GSA against space rent due. If GSA and FCW were able to agree to terms mutually acceptable, and to the benefit of the taxpayer, an amendment to the development agreement to provide for such an offset would require congressional notification as contemplated by the Act.

In closing, if FCW has any specific proposal to amend the development agreement, GSA is available to discuss this proposal with them. If you have any questions, please to contact me at (202) 501-1100, or Mary Gibert, Regional Commissioner, Public Buildings Service, National Capital Region, at (202) 708-5891.

Sincerely,

A handwritten signature in black ink, appearing to read 'NDong', with a stylized flourish extending to the right.

Norman Dong
Commissioner



March 11, 2016

The Honorable Lou Barletta
Chairman, Subcommittee on
Economic Development, Public Buildings,
and Emergency Management
House of Representatives
Washington, DC 20515

The Honorable Eleanor Holmes Norton
Senior Member, Subcommittee on
Economic Development, Public Buildings,
and Emergency Management
House of Representatives
Washington, DC 20515

Dear Chairman Barletta and Congresswoman Norton:

Thank you for your letter dated February 8, 2016, regarding the U.S. General Services Administration's (GSA) response to various requests by Forest City Washington for evaluation of ground rent acceleration at The Yards as additional consideration in potential office space lease procurements.

GSA is currently examining all of the questions and issues in your comprehensive letter. We are giving each of the proposed questions consideration and will respond to you within 60 days, as requested in your letter.

If you have any questions, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "Lisa A. Austin".

Lisa A. Austin
Associate Administrator

**QUESTIONS FOR THE RECORD
FOR
MR. NORMAN DONG
COMMISSIONER, PUBLIC BUILDINGS SERVICE
U.S. GENERAL SERVICES ADMINISTRATION**

**HOUSE COMMITTEE ON TRANSPORTATION & INFRASTRUCTURE SUBCOMMITTEE ON
ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS, AND EMERGENCY MANAGEMENT
“SAVING TAXPAYER DOLLARS BY REDUCING FEDERAL OFFICE SPACE COSTS”
HEARING ON MARCH 1, 2016**

Questions Submitted by the Subcommittee on Economic Development, Public Buildings, and Emergency Management on behalf of Representative Barbara Comstock (R-VA-10):

SUBJECT 1: International Trade Commission building lease:

1) What analysis was carried out by GSA Central Office that resulted in GSA reversing its August 2015 approval of the U.S. International Trade Commission’s (ITC) succeeding lease prospectus? What specifically changed between the approval of the succeeding lease prospectus in late August 2015 and the reversal of approval in early October 2015? Can GSA provide any memos or emails that relate to the decision to reverse?

In fulfilling agency space requirements, the Competition in Contracting Act (CICA) requires GSA to seek full and open competition unless an exception can be justified. Under the General Services Acquisition Regulation, there are leasing exceptions that allow an agency to stay in place. See GSAR Subpart 570. However, at the time that a prospectus is developed, GSA cannot know for certain whether an exception to CICA can be justified and approved. For these reasons, GSA lease prospectuses for other than lease extensions will no longer specify the lease type, such as succeeding, superceding, replacement or new. This change will allow GSA to determine the most appropriate transaction type based on market response.

GSA’s leasing regulation requires GSA to assume that competition is in the Government’s best interest until GSA establishes otherwise. For a succeeding lease, GSA must first issue an advertisement seeking expressions of interest from the market. After placing an advertisement, GSA can negotiate on a sole source basis with the incumbent when GSA receives no other expressions of interest. In addition, GSA may negotiate a succeeding lease when a cost benefit analysis shows that move and replication costs will not be recovered through a competitive procurement. The cost-benefit analysis must compare the rent rates quoted from the market through expressions of interest and the costs of relocation and duplication of tenant improvement against the incumbent’s quoted rent rate. Regardless of whether it will ultimately pursue a full and open competition or a succeeding lease, GSA does not typically release an advertisement until after submitting a prospectus to the House Committee on Transportation and Infrastructure and the Senate Committee on Environment and Public Works for consideration.

2) You stated during the March 1st hearing that GSA wants competition for the ITC just like any other agency. In making this statement, might GSA be overlooking the specific and unique factors associated with the ITC's lease situation? These include the facts that: (1) they have received no appropriation for the renovations associated with the move; (2) they have received an informal proposal from the current landlord that includes a proposed rent reduction of 20%; (3) they will be able to save rent from this proposal during the current lease term; (4) they are not subject to the "reduce the footprint" requirements; (5) they have unique space requirements related to their need for a courtroom complex; and (6) there will be massive disruption to the agency during an extremely active point in time with regard to U.S. trade policy. How is GSA's approach in the best interest of the U.S. taxpayer when every analysis to-date of the ITC's lease situation indicates that the greatest cost savings to the taxpayer will be achieved via a succeeding lease at a reduced rate?

GSA will take into consideration the relocation and duplication costs in a cost benefit analysis to determine whether to seek to enter into a succeeding lease or to move forward with a full and open procurement. If in response to the advertisement, it appears that moving to a new location may cost less than staying in place, then GSA would run a full and open competition. Even in a full and open competition, because GSA wants to capture the true costs to the Government, GSA routinely evaluates the costs of relocation and replication of tenant improvements, when applicable, as would be the case for ITC.

3) During the March 1st hearing, you stated a commitment to take into account the disruption costs to the commission in estimating the cost of moving and replicating new space for the ITC. What factors specifically will GSA consider in estimating the disruption cost to the ITC? Will GSA commit to quantifying those costs? Will GSA commit to incorporating the ITC's estimate of those costs?

GSA collaborated with the ITC in developing its estimate of move and replication costs, which will be accounted for in the cost benefit analysis or price evaluation as discussed above.

4) Will GSA commit to including, as a part of the estimate of the cost of moving and replicating the ITC's space, the lost savings that could be realized by the ITC if GSA had pursued a renegotiation of its current lease as offered by its current landlord?

GSA will fully consider any proposal offered by the current landlord, including any cost savings, as part of its cost-benefit analysis, as discussed above.

5) In a January 2016 report, GAO found that federal leasing costs increase when tenants finance needed improvements to newly leased space over time (GAO-16-188). In a number of examples, GAO noted that agencies lacked sufficient upfront capital and thus incurred significant interest fees, increasing overall costs of the lease. Given that the ITC received zero appropriated funds for a move and that GSA has no budget authority to fund those costs through its Federal Buildings Fund, what guarantee is in place that the ITC would realize the rent savings that would otherwise be realized under a succeeding lease prospectus?

The costs associated with building out new space along with any other cost or rent savings proposed by any offerors in response to the advertisement discussed above will be included and evaluated in the cost benefit analysis. Any lessor who is not the incumbent would need to fully fund and include the move and replication costs as part of the proposed rental rate, as ITC does not have any funding for these expenses. If the result of that analysis shows that the Government cannot expect to recover relocation costs and duplication of costs through competition, GSA will seek approval of a justification for other than full and open competition to enter into a succeeding lease negotiation directly with the incumbent lessor.

6) Currently, the ITC has mission-critical special space in the form of three courtrooms and a main hearing room. The third courtroom was only recently finished in 2012 at a cost of \$3 million to the U.S. taxpayer. The funds for this new courtroom were specifically appropriated by Congress in order to enable the ITC to expedite the adjudication of its intellectual property cases. Will GSA commit to including this cost in the cost of moving and replicating the ITC's space given that the useful life of the new courtroom extends many years into the future?

GSA intends to consider all replication costs, including the cost to replicate the third courtroom, as part of the cost-benefit analysis, or, if appropriate, in its price evaluation of a full and open competition.

7) How can the ITC be certain that a new landlord will spend the amount of money necessary to properly build out the space given that the ITC received no appropriation to move and replicate its space? Will GSA commit to including certain specifications or requirements as requested by the ITC in the lease prospectus, the solicitation, and the request for proposal?

GSA will ensure that all of the ITC's requirements are included in the Request for Lease Proposals (RLP). This is true whether GSA pursues a succeeding lease or a full and open competition. The successful offeror, whether or not it is the incumbent, will be contractually bound to meet the requirements of the RLP and the resulting lease. If the successful offeror later failed to perform, it would be in breach of the lease and GSA would have remedies to either compel performance or to undertake the work and offset associated costs through a deduction from rent paid.

8) What level of savings does GSA consider necessary to justify moving ITC from its current space? Please take into account, among other costs, the cost of disruption to the agency, the loss in rent savings under ITC's current lease, and the \$3 million recently spent to renovate its current space to add a third courtroom. Is the level of savings that GSA considers necessary to justify moving an agency reflected in a written policy or memorandum? If so, will you provide a copy of such policy or memorandum? Is the level of savings considered necessary by GSA to justify moving an agency the same or similar across agencies? If not, why do they differ? Since it is the ITC that is financially responsible for the rent, will GSA commit to taking into account the ITC's view on whether the potential savings justify the cost of moving?

GSA has not established a minimum threshold of savings that must be reached or a standard level of savings that would be necessary to justify moving a tenant. As discussed above, the underlying question is whether, after receiving actual market data to support an analysis, the government can expect to recover relocation costs and duplication costs through competition. Please refer to:

- a. The General Services Administration Acquisition Manual (GSAAM) Subpart 570.402, available at <https://www.acquisition.gov/?q=browsegsam>.
- b. The Leasing Desk Guide Chapter 5, Succeeding Lease, Superseding Lease, available at <http://www.gsa.gov/portal/content/163635>.

9) The ITC's current lease expires in less than 18 months. If GSA forces ITC to move, it is highly unlikely that a new building could be remodeled to fit the ITC's specifications before the current lease expires. Therefore, does GSA acknowledge that the ITC would likely be forced into a lease holdover or extension if they are forced to move?

If GSA cannot support a sole source procurement and the successful proposal after full and open competition is not the one submitted by the incumbent lessor, an extension could be necessary to provide continued housing for the ITC until the new space is constructed according to the requirements contained in the RLP.

SUBJECT 2: Relocation and Consolidation of FBI headquarters:

With regard to the infrastructure surrounding each proposed site:

1) What infrastructure changes would need to be made at the Franconia-Springfield site in order to accommodate the FBI headquarters?

See Draft EIS -- Appendix E, available at www.gsa.gov/fbihqconsolidation (see NEPA tab).

2) What infrastructure changes would need to be made at the Greenbelt site in order to accommodate the FBI headquarters?

See Draft EIS -- Appendix C.

3) What infrastructure changes would need to be made at the Landover site in order to accommodate the FBI headquarters?

See Draft EIS -- Appendix D.

4) What are the strategic benefits associated with relocating the FBI headquarters to the Franconia-Springfield Site?

The sites are now being considered in the context of developer proposal submissions in accordance with the Request for Proposals GSA issued in January of 2016.

It is my understanding that GSA has prescribed dollar figures to each potential site which bidders must use as a “baseline” cost when calculating their bid proposals. It is also my understanding that the base number for the Franconia-Springfield site is significantly larger than that of the other two proposed sites.

5) What factors were used to arrive at this base figure?

For the Franconia-Springfield site, the base figure represents the cost to relocate the current tenants.

6) Is there any flexibility to this base figure associated with the Franconia-Springfield site?

GSA amended the base figure April 9, 2016, and GSA informed the short-listed offerors of this amended base figure.

7) If the state and local governments offer financial assistance with infrastructure or other needs, can this base figure not be modified?

State and local governments may offer financial assistance for infrastructure improvements and Offerors can include this assistance in proposals to provide the most favorable offer to the Federal Government.

SUBJECT 3: Social Security Administration headquarters:

"In March 2014, the Social Security Administration (SSA) Inspector General (IG) identified a significant amount of unused space both at the SSA headquarters as well as other leased buildings nearby (buildings that were not fully occupied). The IG recommended that SSA look to terminate the costly outlying leases and instead consolidate into a building known as Security West adjacent to the headquarters building in Baltimore.

But rather than heed this advice and pursue a long term lease at Security West—which would have locked in a very reasonable rate for square footage—it is my understanding GSA has issued a prospectus for a different space with a square footage rate that doubles that at Security West."

1) Is this a case of the administration adhering to its goal of reducing the footprint?

The prospectus submission implements GSA's priorities of actually reducing the federal footprint and promoting greater competition in the leasing program.

SSA and GSA have aggressively reduced SSA's footprint in the Woodlawn real estate market. Since 2013, GSA has terminated 10 leases in coordination with SSA. These terminations have

resulted in an annual rental savings of \$9,250,000 and represent a square footage reduction of 625,000 RSF.

2) Is it acceptable to reduce the footprint even in cases in which doing so will lead to higher costs?

The contemplated housing plan for the Security West Replacement project implements a reduction of about 362,203 rentable square feet (RSF), which represents a 41% square foot reduction of the current lease. The all-in utilization rate will dramatically improve from 297 to 163 square feet per person. The current lease will expire on October 31, 2018 and GSA has determined to seek full and open competition for the replacement action. In addition to Competition in Contracting Act's requirement for full and open competition, GSA will realize better results for SSA and the taxpayer if these long term requirements (20 years) including updated codes and lease standards are competed.



**Committee on Transportation and Infrastructure
U.S. House of Representatives**

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

April 21, 2016

Christopher P. Bertram, Staff Director

Katherine W. Dedrick, Democratic Staff Director

The Honorable Denise Turner Roth
Administrator
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Administrator Roth:

On April 20, 2016, pursuant to section 3307 of Title 40, United States Code, the Committee on Transportation and Infrastructure met in open session to consider two resolutions included in the General Services Administration's Capital Investment and Leasing Programs.

The Committee continues to work to reduce the cost of federal property and leases. The two resolutions considered for alteration projects address serious health and life safety issues and will consolidate agencies out of leased space into owned space reducing the costs to the taxpayer. The amounts authorized are consistent with existing funding. In total, these resolutions represent more than \$27 million in avoided lease costs.

I have enclosed copies of the resolutions adopted by the Committee on Transportation and Infrastructure on April 20, 2016.

Sincerely,

Bill Shuster
Chairman

Enclosures

cc: The Honorable Peter A. DeFazio, Ranking Member



**Committee on Transportation and Infrastructure
U.S. House of Representatives**

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

AMENDED COMMITTEE RESOLUTION

Christopher P. Bertram, Staff Director

Katherine W. Dedrick, Democratic Staff Director

**ALTERATION
EDWARD J. SCHWARTZ FEDERAL BUILDING AND U.S. COURTHOUSE
SAN DIEGO, CA
PCA-0167-SD16**

Resolved by the Committee on Transportation and Infrastructure of the U.S. House of Representatives, that pursuant to 40 U.S.C. §3307, appropriations are authorized for the design and construction for the reconfiguration and alteration of space in the Edward J. Schwartz Federal Building-Courthouse to backfill vacant space resulting from the opening of the San Diego Courthouse in FY2013, allowing federal tenants to reduce their overall footprint, the relocation of childcare operations currently housed in leased space, and correcting life safety and security deficiencies at an additional design and review cost of \$5,795,000, an estimated additional construction cost of \$49,800,000 and an additional management and inspection cost of \$5,250,000 for an additional total estimated project cost of \$60,845,000, a prospectus for which is attached to and included in this resolution. This resolution amends the resolution adopted by the Committee on September 17, 2014 related to prospectus PCA-0167-SD14.

Provided, that the General Services Administration shall not delegate to any other agency the authority granted by this resolution.

Adopted: April 20, 2016


Bill Shuster, M.C.
Chairman

**AMENDED PROSPECTUS - ALTERATION
EDWARD J. SCHWARTZ FEDERAL BUILDING AND U.S. COURTHOUSE
SAN DIEGO, CA**

Prospectus Number: PCA-0167-SD16
Congressional District: 53

FY2016 Project Summary

Through amended prospectus, the General Services Administration (GSA) proposes design and construction for the reconfiguration and alteration of space in the Edward J. Schwartz Federal Building-Courthouse (FB-CT) to backfill vacancy resulting from the opening of the San Diego Courthouse in FY2013. In addition to recapturing vacant space, the project allows federal tenants to reduce their overall footprint by consolidating their operations in federal space, relocate childcare operations currently housed in leased space, and correct significant life safety and security deficiencies in the facility. Approximately 94,000 rentable square feet will be reconfigured, allowing the Government to release costly leased space reducing the Government's rental payment to the private sector by approximately \$2,723,000 annually.

This prospectus amends Prospectus No. PCA-0167-SD14, to reflect scope changes since the submission of the FY2014 prospectus and to complete work that was not previously approved or funded in FY 2014. Of the \$61,136,000 requested in FY14, GSA received approval for a portion of the proposed project request and apportioned \$19,729,000 of funding as part of its FY2014 Major Repair and Alteration Expenditure Plan.

FY2016 Committee Approval and Appropriation Requested

(Design, ECC and M&I).....\$60,845,000

Major Work Items

Interior construction; security, electrical, fire protection and plumbing systems upgrades; exterior construction

Project Budget

Design and Review (FY 2014)	\$1,997,317
Additional Design and Review	5,795,000
Estimated Construction Cost (ECC) (FY 2014)	16,042,940
Additional ECC.....	49,800,000
Management and Inspection (M&I) (FY 2014).....	1,688,743
Additional M&I	5,250,000
Estimated Total Project Cost (ETPC)*.....	\$80,574,000

*Tenant agencies may fund an additional amount for alterations above the standard normally provided by the GSA.

**AMENDED PROSPECTUS - ALTERATION
EDWARD J. SCHWARTZ FEDERAL BUILDING AND U.S. COURTHOUSE
SAN DIEGO, CA**

Prospectus Number: PCA-0167-SD16
Congressional District: 53

Schedule

Design and Construction

Start

FY2016

End

FY2020

Building

The 895,247 gross square foot (rsf) Edward J. Schwartz Federal Building and US Courthouse, at 880 Front Street in downtown San Diego, was built in 1973. It consists of two adjacent structures: a six-story federal office wing, a five-story court wing, and underground parking and basement offices. The building's two wings share an upper basement and are connected by a bridge between the fifth and sixth floors.

Tenant Agencies

Judiciary, U.S. Department of Homeland Security, Probation; U.S. Department of Justice, U.S. Treasury Department, U.S. Environmental Protection Agency, GSA, and Childcare.

Proposed Project

Approximately 67,000 RSF of vacant space will be built out for backfill occupancy by the Executive Office for Immigration Review (EOIR), the U.S. Coast Guard, Probation, Grand Jury, and the U.S. Environmental Protection Agency (EPA). Two public restrooms will be remodeled for compliance with the Architectural Barriers Act Accessibility Standard (ABAAS). Security upgrades, including hardening on several facades and the installation of bollards and an anti-ram barrier at the entrance to the garage will be undertaken. Building system upgrades including new automatic transfer switches, a new electric fire pump, new domestic water shut-off valves, a new emergency generator and new quick response fire sprinkler heads will be installed. Precast concrete panels on the south elevation of the building's office wing will be cleaned and sealed. Approximately 13,000 rsf of space will also be built out for a childcare center currently housed in leased space. In addition, approximately 5,000 rsf of vacant storage will be returned to parking for government vehicles in the upper basement and 10,000 rsf of basement space will be prepared for tenant occupancy.

**AMENDED PROSPECTUS - ALTERATION
EDWARD J. SCHWARTZ FEDERAL BUILDING AND U.S. COURTHOUSE
SAN DIEGO, CA**

Prospectus Number: PCA-0167-SD16
Congressional District: 53

Major Work Items

Plumbing Upgrade/ABAAS	\$1,511,000
Blast Mitigation	3,452,000
Site Security Upgrade	1,300,000
Fire Protection Upgrade	1,372,000
Electrical Upgrade	4,623,000
Interior Construction	37,132,000
Exterior Construction	<u>410,000</u>
Total ECC	\$49,800,000

Justification

In FY2014, GSA submitted Prospectus Number PCA-0167-SD14, proposing a \$61,136,000 repair and alteration project to alter vacant space, consolidate multiple agencies, and upgrade building systems. In the absence of full funding for the FY2014 Capital Investment and Leasing Program, GSA's FY2014 Expenditure Plan for Major Repairs and Alterations Program funded the project at \$19,729,000. The Senate Committee on Environment and Public Works and the House Committee on Transportation and Infrastructure approved the reduced scope and funding. This amended prospectus allows GSA to accomplish scope that was not funded in FY2014 and to undertake additional scope items including conversion of vacant storage space, childcare and consolidate multiple agencies.

The project will allow GSA to backfill approximately 94,000 rsf vacated by certain District Court Judges and staff, and the Court clerk's operations when they moved to the new San Diego Courthouse in FY2013 as well as additional space vacated by the Internal Revenue Service when they relocated to Courthouse.

Currently the building does not meet blast and security standards. In addition, failure to repair or replace the outdated and inefficient building systems will cause operating costs to continue to increase and would likely lead to costly system failures. Further deterioration of the building's systems will make it difficult to backfill the space vacated by tenants that relocated to the San Diego Courthouse Annex.

Summary of Energy Compliance

This project will be designed to conform to requirements of the Facilities Standards for the Public Buildings Service and will implement strategies to meet the Guiding Principles for High Performance and Sustainable Buildings. GSA encourages design opportunities to increase energy and water efficiency above the minimum performance criteria.

**AMENDED PROSPECTUS - ALTERATION
EDWARD J. SCHWARTZ FEDERAL BUILDING AND U.S. COURTHOUSE
SAN DIEGO, CA**

Prospectus Number: PCA-0167-SD16
Congressional District: 53

Prior Appropriations

Prior Appropriations			
Public Law	Fiscal Year	Amount	Purpose
113-76	2014	\$19,729,000	Design and Construction
Appropriations to Date		\$19,729,00	

Prior Committee Approvals

Prior Committee Approvals			
Committee	Date	Amount	Purpose
House T&I	9/17/2014	\$19,729,000	Design = \$1,997,317 ECC = \$16,042,940 M&I = \$1,688,743 (ICE consolidation and backfill)
Senate EPW	9/18/2014	\$19,729,000	Design = \$1,997,317 ECC = \$16,042,940 M&I = \$1,688,743 (ICE consolidation and additional building improvements)
Approvals to Date		\$19,729,000	

**AMENDED PROSPECTUS - ALTERATION
EDWARD J. SCHWARTZ FEDERAL BUILDING AND U.S. COURTHOUSE
SAN DIEGO, CA**

Prospectus Number: PCA-0167-SD16
Congressional District: 53

Alternatives Considered (30-year, present value cost analysis)

New Construction.....	\$282,604,000
Alteration.....	\$262,434,000
Leasing.....	\$487,736,000

The 30-year, present value cost of alteration is \$20,170,000 less than the cost of new construction with an equivalent annual cost advantages of \$1,152,000.

Recommendation

ALTERATION

**AMENDED PROSPECTUS - ALTERATION
EDWARD J. SCHWARTZ FEDERAL BUILDING AND U.S. COURTHOUSE
SAN DIEGO, CA**

Prospectus Number: PCA-0167-SD16
Congressional District: 53

Certification of Need

The proposed project is the best solution to meet a validated Government need.

Submitted at Washington, DC, on February 2, 2015

Recommended: 
Commissioner, Public Buildings Service

Approved: 
Administrator, General Services Administration

(b) (7)(F)

(b) (7) (F)

(b) (7) (F)



**Committee on Transportation and Infrastructure
U.S. House of Representatives**

**Bill Shuster
Chairman**

Washington, DC 20515

**Peter A. DeFazio
Ranking Member**

Christopher P. Bertram, Staff Director

COMMITTEE RESOLUTION

Katherine W. Dedrick, Democratic Staff Director

**ALTERATION
DISTRICT COURTHOUSE
PENSACOLA, FL
PFL-2245-PE15**

Resolved by the Committee on Transportation and Infrastructure of the U.S. House of Representatives, that pursuant to 40 U.S.C. §3307, appropriations are authorized for a repair and alteration project to remediate mold, eliminate water infiltration, replace the building façade, and undertake system and site upgrades at the Pensacola District Courthouse located at 1 North Palafox Street in Pensacola, Florida at a design cost of \$2,673,000, an estimated construction cost of \$25,259,000 and a management and inspection cost of \$2,849,000 for a total estimated project cost of \$30,781,000, a prospectus for which is attached to and included in this resolution.

Provided, that the General Services Administration shall not delegate to any other agency the authority granted by this resolution.

Adopted: April 20, 2016

**Bill Shuster, M.C.
Chairman**

**PROSPECTUS – ALTERATION
DISTRICT COURTHOUSE
PENSACOLA, FL**

Prospectus Number: PFL-2245-PE15
Congressional District: 1

FY 2016 Project Summary

The General Services Administration (GSA) proposes a repair and alteration project to remediate mold, eliminate water infiltration, replace the building facade, and undertake system and site upgrades at the Pensacola District Courthouse located at 1 North Palafox Street in Pensacola, FL (the "District Courthouse").

The District Courthouse is a leased facility that was constructed on land owned by the City of Pensacola and made available to GSA's selected developer pursuant to a Ground Lease. It was constructed for use by the Courts and leased by GSA since 1997. The firm term of the current space lease between GSA and the owner of the courthouse, Palafox Street Associates, LP, expires on July 31, 2017 (the "Courthouse Lease"). GSA has an unconditional right to accept an irrevocable Offer of Donation from the City of Pensacola to take fee simple ownership of the site and improvements at the end of the current 20-year Courthouse Lease term. GSA plans to acquire ownership of the site and improvements by accepting the Offer of Donation, thereby taking ownership from the City of Pensacola upon expiration of the initial term of the Courthouse Lease.

FY 2016 Committee Approval Requested

(Design, Construction, Management and Inspection)\$30,781,000

FY 2016 Appropriation Requested¹\$0

Major Work Items

Exterior construction; interior construction; mold abatement; roof replacement; heating, ventilating and air conditioning (HVAC)/mechanical, life safety/emergency and plumbing systems upgrades; site work; security upgrades; demolition.

Project Budget

Design	\$2,673,000
Estimated Construction Cost (ECC)	\$25,259,000
Management and Inspection (M&I).....	<u>\$2,849,000</u>

¹ Although no funds are being requested in this prospectus, approval of the prospectus is needed for this repair and alteration project. Concurrently, GSA will request approval to reprogram previously appropriated project funds to pay for this proposed repair and alteration project.

**PROSPECTUS - ALTERATION
DISTRICT COURTHOUSE
PENSACOLA, FL**

Prospectus Number: PFL-2245-PE15
Congressional District: 1

Estimated Total Project Cost (ETPC)*.....\$30,781,000

*Tenant agencies may fund an additional amount for tenant improvements above the standard normally provided by the GSA.

<u>Schedule</u>	<u>Start</u>	<u>End</u>
Design	FY 2016	FY 2016
Construction	FY 2016	FY 2018

Building

The District Courthouse in Pensacola is a five-story leased building built for use by the Federal judiciary and occupied in August 1997 under a 20-year, below-prospectus lease (including two options of 5 additional years each). The building is owned by GSA's current Lessor, Palafox Street Associates, and was constructed on land owned by the City of Pensacola pursuant to a Ground Lease between the City of Pensacola and the building's developer. The ground lease agreement is coterminous with the Courthouse Lease. This Court's function in this building is in conjunction with the court and court-related functions housed in the federally owned Winston E. Amow U.S. Courthouse, located at 100 N. Palafox Street. The Amow Courthouse is 79,840 rentable square feet (RSF) and provides 5 inside parking spaces and 22 outside surface parking spaces.

The Courthouse Lease expires on July 31, 2017. Upon expiration of the Courthouse Lease, GSA has the right, through an Offer of Donation provided from the City of Pensacola, to assume ownership of the underlying land and improvements. With the end of the current lease term nearing, GSA plans to accept the donation, enabling the Government to take ownership of the District Courthouse land and improvements from the City, at no cost.

Tenant Agencies

Judiciary, U.S. Department of Justice - Office of the U.S Attorney, U.S. Department of Justice - Marshals Service, U.S. Congress - Senate, GSA

Proposed Project

GSA proposes alterations to the District Courthouse that will correct the water intrusion issues in the building by replacing the building's facade, installing a new standing seam metal roof system, repairing structural damage to the building caused by the water

**PROSPECTUS – ALTERATION
DISTRICT COURTHOUSE
PENSACOLA, FL**

Prospectus Number: PFL-2245-PE15

Congressional District: 1

intrusion, and completely abating the presence of mold created by the water intrusion. The new building envelope will be weathertight and meet the State of Florida hurricane requirements. GSA will also install a new security blast protection system to the exterior during the facade repairs consistent with current security standards. Interior finishes throughout the building damaged by the water intrusion will also be repaired or replaced. In addition, the project will modernize the outdated fire safety system and the heating ventilating and air conditioning (HVAC) system by adding additional variable air volume boxes and a new building automation system to better control the interior humidity. The restrooms in the building will also be upgraded, including the installation of floor drains, replacement of wall finishes, and Architectural Barriers Act Accessibility Standard compliant unisex restrooms will be installed on each floor. Grounds and approaches will be repaired after facade demolition and replacement. Parking will be repaved and waterproofing and drainage will be installed on the site.

Major Work Items

Superstructure/Exterior Repairs	\$9,750,000
Interior Construction & Finishes	5,090,000
HVAC Upgrades	2,181,000
Mold Abatement	2,078,000
Roof Replacement	1,485,000
Fire Protection Upgrades	1,327,000
Electrical Upgrades	1,308,000
Plumbing Upgrades	798,000
Site Repairs/Improvements	760,000
Demolition	<u>482,000</u>
Total ECC	\$25,259,000

Justification

The existing leased District Courthouse has experienced water intrusion issues dating back to initial occupancy. GSA under the Courthouse Lease is responsible for all maintenance and capital improvements, and has made numerous repairs over the term of the lease to attempt to resolve these issues. However, the selective repairs have not been able to adequately correct the building deficiencies, and water intrusion issues persisted. GSA identified significant water intrusion and mold issues in 2014, and, as a result, GSA is pursuing a comprehensive solution. Due primarily to the health-related concerns reported by building occupants, and the limited ability to move occupants within the building during the proposed renovation without disrupting agency missions, GSA

**PROSPECTUS – ALTERATION
DISTRICT COURTHOUSE
PENSACOLA, FL**

Prospectus Number: PFL-2245-PE15
Congressional District: 1

relocated all building tenants out of the leased District Courthouse and into a 14,946 rentable square foot lease in June 2015 and the Arnow Courthouse. The 1 N. Palafox Street courthouse is currently vacant and will remain so for the duration of the renovation project.

Summary of Energy Compliance

This project will be designed to conform to requirements of the Facilities Standards for the Public Buildings Service and will implement strategies to meet the Guiding Principles for High Performance and Sustainable Buildings. GSA encourages design opportunities to increase energy and water efficiency above the minimum performance criteria.

Prior Appropriations

N/A

Prior Committee Approvals

N/A

Prior Prospectus-Level Projects in Building (past 10 years):

N/A

Alternatives Considered (30-year, present value cost analysis)

Alteration:	\$56,120,271
New Construction:	\$53,371,076
Lease	\$100,838,333

GSA has determined that taking ownership of the courthouse and executing the repair and alterations project identified in this prospectus is the most efficient means of housing the U.S. District Courts in Pensacola, FL. The 30-year, present value cost of alteration is \$2,749,195 more than the cost of new construction with an equivalent annual cost disadvantage of \$147,610, and \$44,718,062 less than the cost of a lease with an equivalent annual cost advantage of \$2,548,623. At this time, the GSA Federal Building Fund has the necessary funds available to support the limited alteration of the District Courthouse allowing for re-occupancy of the District Courthouse. Utilizing existing Federal Building Fund resources, the Alteration alternative also provides a long-term housing solution for building occupants more quickly than the New Construction alternative.

GSA

PBS

**PROSPECTUS - ALTERATION
DISTRICT COURTHOUSE
PENSACOLA, FL**

Prospectus Number: PFL-2245-PE15
Congressional District: 1

Recommendation

ALTERATION

Certification of Need

The proposed project is the best solution to meet a validated Government need.

Submitted at Washington, DC, on March 31, 2016

Recommended: 

Commissioner, Public Buildings Service

Approved: 

Administrator, General Services Administration



Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

July 13, 2016

Christopher P. Bertram, Staff Director

Katherine W. Dedrick, Democratic Staff Director

Mr. Norman Dong
Commissioner
Public Buildings Service
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Commissioner Dong:

As part of the General Services Administration's Fiscal Year 2016 Capital Investment and Leasing Program, a prospectus for the modernization of the Herbert C. Hoover Building in Washington, D.C. was submitted for approval and is pending before the Committee. The purpose of the proposed project is to renovate and reconfigure the building, improve space utilization, and consolidate more agencies into this 1.9-million-usable-square-foot building to reduce taxpayer costs. We are requesting you submit a housing plan for the prospectus that indicates the Federal Trade Commission (FTC) will relocate from the Apex Building to the Hoover Building.

As you are aware, the Committee has passed a previous resolution exploring the relocation of the Federal Trade Commission headquarters currently located at 600 Pennsylvania Avenue in Washington D.C. (Apex building). The Apex building is an inefficient building for modern office space, with only 52% of the gross square footage usable for FTC operations, and will require extensive renovations in the future. The National Gallery of Art (NGA), which sits directly across the street from the Apex building, requires additional space to consolidate its operations currently housed in leased space. Consolidating NGA's leased space into government owned space would provide significant savings. In addition, the Apex Building's future renovation costs would be borne by NGA supported private donations thus saving taxpayers an estimated one hundred and fifty million dollars.

Given this, we believe relocating the FTC has the potential to reduce taxpayer costs over the long term. We understand that a federal tenant agency has not yet been identified for approximately 200,000 square feet of space included in the later phases of the Hoover Building modernization project. This would be more than enough space to house the FTC headquarters functions and co-locate the agency with the headquarters of the Department of Commerce.

To this end, we request that you provide the Committee with a housing plan for the prospectus submitted for the modernization of the Herbert C. Hoover Building that includes the relocation of the operations of the FTC headquarters currently housed at 600 Pennsylvania Avenue in Washington, D.C.

Sincerely,



Bill Shuster
Chairman
Committee on Transportation
and Infrastructure



John Mica
Member
Committee on Transportation
and Infrastructure



Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

July 13, 2016

Christopher P. Bertram, Staff Director

Katherine W. Dedrick, Democratic Staff Director

Mr. Norman Dong
Commissioner
Public Buildings Service
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Commissioner Dong:

As part of the General Services Administration's Fiscal Year 2016 Capital Investment and Leasing Program, a prospectus for the modernization of the Herbert C. Hoover Building in Washington, D.C. was submitted for approval and is pending before the Committee. The purpose of the proposed project is to renovate and reconfigure the building, improve space utilization, and consolidate more agencies into this 1.9-million-usable-square-foot building to reduce taxpayer costs. We are requesting you submit a housing plan for the prospectus that indicates the Federal Trade Commission (FTC) will relocate from the Apex Building to the Hoover Building.

As you are aware, the Committee has passed a previous resolution exploring the relocation of the Federal Trade Commission headquarters currently located at 600 Pennsylvania Avenue in Washington D.C. (Apex building). The Apex building is an inefficient building for modern office space, with only 52% of the gross square footage usable for FTC operations, and will require extensive renovations in the future. The National Gallery of Art (NGA), which sits directly across the street from the Apex building, requires additional space to consolidate its operations currently housed in leased space. Consolidating NGA's leased space into government owned space would provide significant savings. In addition, the Apex Building's future renovation costs would be borne by NGA supported private donations thus saving taxpayers an estimated one hundred and fifty million dollars.

Given this, we believe relocating the FTC has the potential to reduce taxpayer costs over the long term. We understand that a federal tenant agency has not yet been identified for approximately 200,000 square feet of space included in the later phases of the Hoover Building modernization project. This would be more than enough space to house the FTC headquarters functions and co-locate the agency with the headquarters of the Department of Commerce.

To this end, we request that you provide the Committee with a housing plan for the prospectus submitted for the modernization of the Herbert C. Hoover Building that includes the relocation of the operations of the FTC headquarters currently housed at 600 Pennsylvania Avenue in Washington, D.C.

Sincerely,



Bill Shuster
Chairman
Committee on Transportation
and Infrastructure



John Mica
Member
Committee on Transportation
and Infrastructure

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

July 21, 2016

The Honorable Denise Turner Roth
Administrator
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Ms. Roth:

The Hatch Act prohibits using money derived from the United States Treasury to pay for costs associated with political activity by executive branch employees.¹ More specifically, the Committee's long-held position is that taxpayers "should . . . not pay the travel expenses of cabinet and other senior officials to fly across the country" for political purposes."² The President recently made his first campaign appearance at an event in North Carolina,³ and as the election approaches, it is likely that he and other senior administration officials will participate in campaign events across the country.

The Hatch Act regulations define "political activity" as "an activity directed towards the success or failure of a political party, candidate for partisan political office, or partisan political group."⁴ It is not always clear, however, whether an event is political or official in nature. We are writing to determine how your agency or your office makes decisions about how to structure official trips to comply with the Hatch Act and other applicable laws. Further complicating the matter is that some trips may involve both political and official activities. The costs associated with the political components of a senior official's mixed trip may not be paid using funds from the United States Treasury,⁵ so it is necessary to carefully track the official's time to determine what portion of the travel costs must be reimbursed.

¹ 5 U.S.C. § 7324 (b)(1).

² H. Comm. on Oversight & Gov't Reform Democratic Staff Report, *The Activities of the White House Office of Political Affairs*, 110th Cong. (Oct. 2008), available at <http://oversight-archive.waxman.house.gov/documents/20081015105434.pdf>.

³ Amy Chozick and Michael D. Shear, *Obama Joins Hillary Clinton on Stump, Saying She 'Has Been Tested'*, N.Y. TIMES, July 5, 2016.

⁴ 5 C.F.R. § 734.101.

⁵ 5 U.S.C. § 7324 (b)(1).

To help the Committee understand how your agency manages these responsibilities, please provide written responses to the following questions as soon as possible, but no later than August 4, 2016:

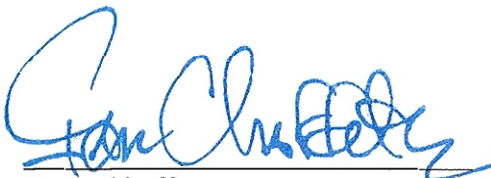
1. How does your agency ensure compliance with the Hatch Act's restrictions on political travel?
2. What is the formula for apportioning costs incurred during travel that has both official and political components?
3. How do you and your staff handle travel requests from other government officials or offices, whether it be the White House, a Member of Congress, or a separate agency, on a procedural basis?
4. What political events have Presidentially-appointed Senate confirmed (PAS) officials in your agency traveled to in 2016, to date? Please identify the event and the agency participants.
5. What political events are PAS officials in your agency scheduled to attend in 2016 and are any of those events expected to have mixed travel? Please identify the event and the agency participants.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X.

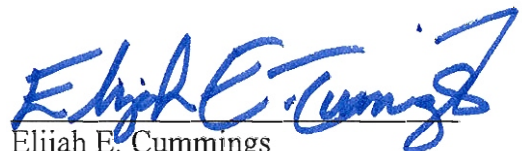
Please deliver your responses to the Majority Staff Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building. The Committee prefers to receive all documents in electronic format. An attachment to this letter provides additional instructions for responding to the Committee's requests.

Thank you for your attention to this matter. Please have your staff contact Jonathan Skladany of the Committee's Majority staff at (202) 225-5074 or Krista Boyd of the Minority staff at (202) 225-5051 with any questions about this matter.

Sincerely,



Jason Chaffetz
Chairman



Elijah E. Cummings
Ranking Member

Enclosure

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
 - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
 - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,
CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE,
DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,
INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.
6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.
17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.

19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.
3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term “referring or relating,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term “employee” means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.



August 3, 2016

The Honorable Jason Chaffetz
Chairman
Committee on Oversight and
Government Reform
House of Representatives
Washington, DC 20515

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform
House of Representatives
Washington, DC 20515

Dear Chairman Chaffetz and Ranking Member Cummings:

Thank you for your letter dated July 21, 2016, regarding travel and political activity from January 1, 2016, to the present.

The U.S. General Services Administration (GSA) understands your concern about the use of taxpayer funds to further partisan political activities. This is more than just an issue of expenditure of taxpayer funds; it is also about ensuring compliance with the law and ensuring that partisan politics do not interfere with the business of the American people.

Last year, and most recently this year, all senior GSA officials received ethics training and guidance that included extensive coverage of the Hatch Act. In addition, as part of the agency's top-to-bottom review, GSA instituted internal reforms focused on travel by agency personnel. One important reform prevents anyone at GSA, including the Administrator, from authorizing his or her own travel. Each trip must be approved by at least one other senior agency official.

Please be assured that GSA personnel understand the limits on their partisan political activities and fully comply with all requirements. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in black ink, appearing to read "Lisa A. Austin".

Lisa A. Austin
Associate Administrator



August 5, 2016

The Honorable Jason Chaffetz
Chairman
Committee on Oversight and
Government Reform
House of Representatives
Washington, DC 20515

The Honorable Mark Meadows
Chairman
Subcommittee on Government Operations
Committee on Oversight and
Government Reform
House of Representatives
Washington, DC 20515

Chairman Chaffetz and Chairman Meadows:

Thank you for your letter dated July 22, 2016, regarding Computers for Learning (CFL). Administrator Denise Turner Roth has asked that I respond to your letter. The U.S. General Services Administration (GSA) shares your interest in making modern computer technology available to American children to ensure that they possess the skills needed to compete in the 21st century.

Executive Order (EO) 12999, which implements the CFL program, cites three legal authorities under which Federal assets may be transferred to schools and educational non-profit organizations. The first and most widely used authority is 15 USC § 3710(i), commonly known as "The Stevenson-Wydler Technology Innovation Act of 1980" or "Stevenson-Wydler." This statute authorizes all Federal agencies to transfer research equipment, including computers and peripheral equipment, directly to an educational institution or a nonprofit organization, without GSA's approval or oversight. The second authority is GSA's Federal Surplus Personal Property Donation Program, under 40 USC § 549, (N.B. this provision was recodified in 2002 under Public Law 107-217, and differs from the Title 40 citation referenced in EO 12999). Transfers made under this authority account for 3 percent of total transfers made through the CFL program.

Due to the minimal use of this authority, GSA's response focuses on transfers made through the Stevenson-Wydler authority. The third authority includes provisions in the National Defense Authorization Act for Fiscal Year 1996, Public Law 104-106. These are U.S. Department of Defense authorities that are outside the scope of GSA's purview, and therefore are not discussed in this response.

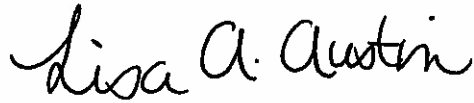
Since fiscal year 2000, GSA has supported the CFL program by hosting a website. Use of the CFL website is encouraged as a tool for making computer and peripheral equipment transfers; however, use of the website is not mandatory. GSA's information indicates that the majority of CFL transfers (in terms of Original Acquisition Cost [OAC]) happen outside the CFL website. The authority to transfer CFL equipment remains with the owning agency regardless of whether they utilize the CFL website. The website lists available equipment and allows schools and educational nonprofit organizations to request property from the Federal agencies who have reported useful computer equipment as excess to their needs. Potential recipients register for access to the CFL website by uploading eligibility information. Registering allows potential recipients to self-certify their eligibility and to view and request available equipment. At an agency's discretion, an agency can access both the U.S. Department of Education's and U.S. Department of Treasury - Internal Revenue Service's websites to further research and verify the eligibility of potential CFL recipients before determining that a school or educational nonprofit organization is an appropriate CFL equipment recipient. Guidance encouraging agencies to verify potential recipients is available on the CFL website.

GSA also collects and reports data on an annual basis, under 40 USC § 529, including equipment transfers to non-Federal entities. Agency transfers made under EO 12999 must be reported pursuant to this requirement. Last year, Federal agencies directly transferred computers and peripheral equipment valued at approximately \$49.7 million (OAC) using the CFL website. Agencies also directly transferred computers and peripheral equipment valued at approximately \$75.2 million (OAC) outside the CFL website. These reports are included for your review (see answer to question 4). The data in these reports is self-reported by agencies. GSA does not audit the data other than to attempt to correct obvious errors.

Thank you for your oversight of the Government's efforts to ensure that the nation's youth are prepared to compete in and contribute to today's increasingly technological economy and society. The answers to your seven inquiries are contained on the enclosed thumb drives. GSA is happy to provide a briefing on this issue or answer any additional questions you may have.

If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in black ink that reads "Lisa A. Austin". The signature is written in a cursive, flowing style.

Lisa A. Austin
Associate Administrator

cc: The Honorable Elijah E. Cummings
The Honorable Gerald E. Connolly

HAROLD ROGERS, KENTUCKY, CHAIRMAN

RODNEY P. FRELINGHUYSEN, NEW JERSEY
ROBERT B. ADERHOLT, ALABAMA
KAY GRANGER, TEXAS
MICHAEL K. SIMPSON, IDAHO
JOHN ABNEY CULBERSON, TEXAS
ANDER CRENSHAW, FLORIDA
JOHN R. CARTER, TEXAS
KEN CALVERT, CALIFORNIA
TOM COLE, OKLAHOMA
MARIO DIAZ-BALART, FLORIDA
CHARLES W. DENT, PENNSYLVANIA
TOM GRAVES, GEORGIA
KEVIN YODER, KANSAS
STEVE WOMACK, ARKANSAS
JEFF FORTENBERRY, NEBRASKA
THOMAS J. ROONEY, FLORIDA
CHARLES J. FLEISCHMANN, TENNESSEE
JAIME HERRERA BEUTLER, WASHINGTON
DAVID P. JOYCE, OHIO
DAVID G. VALADAO, CALIFORNIA
ANDY HARRIS, MARYLAND
MARTHA ROBY, ALABAMA
MARK E. AMODEI, NEVADA
CHRIS STEWART, UTAH
E. SCOTT RIGELL, VIRGINIA
DAVID W. JOLLY, FLORIDA
DAVID YOUNG, IDAHO
EVAN H. JENKINS, WEST VIRGINIA
STEVEN M. PALAZZO, MISSISSIPPI

Congress of the United States
House of Representatives
Committee on Appropriations
Washington, DC 20515-6015

NITA M. LOWEY, NEW YORK
MARCY KAPTUR, OHIO
PETER J. VISCLOSKEY, INDIANA
JOSE E. SERRANO, NEW YORK
ROSA L. DELAUNO, CONNECTICUT
DAVID E. PRICE, NORTH CAROLINA
LUCILLE ROYBAL-ALLARD, CALIFORNIA
SAM FARR, CALIFORNIA
SANFORD D. BISHOP, JR., GEORGIA
BARBARA LEE, CALIFORNIA
MICHAEL M. HONDA, CALIFORNIA
BETTY MCCOLLUM, MINNESOTA
STEVE ISRAEL, NEW YORK
TIM RYAN, OHIO
C. A. DUTCH RUPPERSBERGER, MARYLAND
DEBBIE VASSERMAN SCHULTZ, FLORIDA
HENRY CUELLAR, TEXAS
CHELLIE PINGREE, MAINE
MIKE QUIGLEY, ILLINOIS
DEREK KILMER, WASHINGTON

WILLIAM E. SMITH
CLERK AND STAFF DIRECTOR

TELEPHONE
(202) 225-2771

August 10, 2016

Denise Turner Roth
Administrator
General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Ms. Roth:

Authorization is hereby granted to Ander Crenshaw a member of the Committee, and Ariana Sarar, a staff member of the Committee, to travel to Pensacola, Florida on or about August 21 through 22, 2016. The purpose of the trip is to tour the U.S. District Court in Pensacola, which is of interest to the Subcommittee on Financial Services and General Government. Mr. Crenshaw will be departing from and returning to his district office in Jacksonville, Florida and Ms. Sarar will be departing from and returning to Washington, D.C.

Per diem expenses of \$123.00 per day, or the rate specified for High Cost Geographical Areas, whichever is higher, plus transportation and other authorized costs, shall be paid from appropriations available under Public Law 83-207 (31 U.S.C. 1108(g)).

It would be appreciated if you will have someone assist in making whatever arrangements are necessary for this travel. The travel will be conducted via commercial carrier.

Sincerely,



Harold Rogers
Chairman



December 28, 2016

The Honorable Peter DeFazio
Ranking Member
Subcommittee on Economic Development,
Public Buildings, and Emergency Management
Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

Dear Representative DeFazio:

Thank you for your letter dated October 20, 2016, in which you expressed concerns over the manner in which the U.S. General Services Administration (GSA) is conducting the lease procurement for the U.S. Environmental Protection Agency's (EPA) Region 8 Headquarters in Denver, Colorado. As I indicated in my letter dated November 8, 2016, your inquiry prompted a review of this procurement to look at the issues you raised. Specifically, you asked for an explanation of GSA's procurement approach and assurance that GSA's actions are compliant with its regulatory requirements and will maximize competition. We assure you that GSA's actions in awarding a succeeding lease are compliant with procurement statutes, regulations, and guidelines within the prospectus approvals, and are in the best interests of the market and the taxpayers.

In your letter, two specific requirements were highlighted as concerns and seen as potentially limiting of competition, namely, the delineated area and the proximity to light rail. Executive Order (EO) 12072 requires Federal agencies procuring space in urban areas to first consider central business districts and adjacent areas of similar character, including other specific areas that may be recommended by local officials. Accordingly, GSA developed the delineated area for this procurement in conjunction with EPA and City of Denver officials to ensure that GSA met EPA's mission requirements and complied with EO 12072. A market survey was also conducted to identify potentially available properties which could meet EPA's minimum requirements. After these efforts and consultations, GSA established a broad delineated area, including business districts outside of the City of Denver's defined central business district. The boundaries of the delineated area were published and included in GSA's prospectus, PCO-08-DE16, submitted to both the U.S. House of Representatives Committee on Transportation and Infrastructure and the U.S. Senate Committee on Environment and Public Works.

Resolutions from both Committees were received by GSA on March 2, 2016 and January 20, 2016, respectively, and both resolutions required the delineated area of the procurement be identical to the delineated area identified in the prospectus unless the Administrator of the General Services Administrator provided an explanatory statement to both Committees. GSA acted in accordance with the prospectus and resolutions and through the market survey and advertisement, identified competitors within the delineated area.

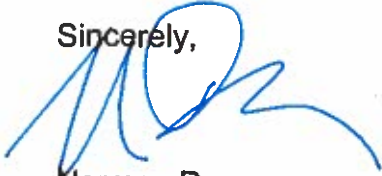
In addition to the prospectus, the solicitation included additional requirements for this procurement including both light rail and bus line accessibility. The light rail and bus line requirements were specifically tailored to EPA's justified needs and do not adversely affect competition within the delineated area. Based upon market research current at the time that the delineated area was established, all of the potentially acceptable blocks of available space within the delineated area were also within the 1,320 walkable linear feet (wlf) distance to light rail and bus lines. Accordingly, the requirement that offered space be located within 1,320 wlf of light rail had no effect on the potential competitive field within the delineated area.

When conducting lease procurements, GSA makes every reasonable effort to maximize competition through market surveys, advertisements, and conducting full and open competitions. There are circumstances, however, that may lead GSA to conclude that the marketplace and the taxpayers are best served by utilization of an exception to competition. The request for expressions of interest provides an opportunity for potential offerors to respond to GSA's requirements and GSA to consider those responses when determining the procurement approach that is in the Federal Government's best interests. In this situation, multiple expressions of interest were received from properties within the delineated area. As noted in the advertisement and in accordance with the Federal Acquisition Regulation and the GSA Acquisition Manual, GSA informed the marketplace that a potential existed for a succeeding lease and that the determination to proceed in that direction would be justified, based on a cost-benefit analysis utilizing the rates proposed by entities responding to the advertisement with expressions of interest. In this case, the analysis justified entering into negotiations for a succeeding lease.

In closing, GSA conducted this procurement in accordance with all applicable procurement laws and regulations, as well as EPA's mission requirements and the Committee Resolutions from the U.S. Senate Committee on Environment and Public Works and the U.S. House of Representatives Committee on Transportation and Infrastructure.

If you have any additional questions or concerns, please contact me at (202) 501-1100.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Norman Dong', with a stylized flourish extending to the right.

Norman Dong
Commissioner



Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

October 20, 2016

Christopher P. Bertram, Staff Director

Katherine W. Dedrick, Democratic Staff Director

Mr. Norman Dong
Commissioner
Public Buildings Service
U.S. General Services Administration
1800 F Street, NW
Washington, D.C. 20405

Dear Commissioner Dong:

We write to express our concerns about the manner in which the General Services Administration (GSA) is conducting its solicitation for a replacement lease for the Environmental Protection Agency's (EPA) office space in downtown Denver, Colorado. We would like an explanation of GSA's approach to this procurement and assurance that it is consistent both with the GSA's regulatory requirements and stated objectives to conduct a procurement process that ensures maximum competition. We are especially concerned because GSA has indicated to at least one potential bidder that GSA intends to pursue a sole-source succeeding lease. **We urge you to suspend any award of the replacement lease until you have addressed these concerns.**

On October 23, 2015, GSA issued Prospectus No. PCO-08-DE16 proposing a replacement lease of up to 176,000 rentable square feet (RSF) for the EPA Region 8 Headquarters. The EPA Headquarters is currently located at 1595 Wynkoop Street, Denver, CO. According to the Prospectus, the replacement lease is intended to provide continued housing for EPA, and to improve the agency office and overall utilization rates. The Prospectus states that the proposed delineated area should include the Platte River to the North, the Intersection of Broadway Street and Speer Boulevard to the South, Broadway Street to the East and Speer Boulevard to the West.

A solicitation notice issued to fulfill this requirement stated additional requirements beyond those enumerated in the Prospectus. In particular, the solicitation notice set forth the Light Rail requirement defining it as follows: "offered buildings must be located within 1,320 walkable linear feet from a light rail station measured along accessibility compliant, paved pedestrian pathways from a main entrance of the offered building to the accessibility compliant entrance to the light rail station."

In December 2015 and January 2016, Members of Congress presented inquiries to GSA regarding the restrictive delineated Area for the EPA procurement, focusing on the fact that this restricted delineated area contravened GSA's recently stated policy goal of broadening delineation areas to increase competition for leases. At a March 1, 2016 hearing before the House Committee on

Transportation and Infrastructure Subcommittee on Economic Development, Public Buildings, and Emergency Management, you testified about this policy. You testified: "To get the best rates for our tenants and for the taxpayer, we need to maximize the amount of competition in our leasing activity . . . To get the best deal for federal agencies and the American taxpayer, GSA is broadening the delineated area for leases in order to increase competition in our lease procurements." In spite of that stated policy, GSA excluded at least one viable building which is located one block outside of the eastern boundary of the established delineated area and indicated that the building would not be considered for the EPA procurement.

In addition, there are anecdotal reports from local Denver realtors that the delineated area excludes a portion of downtown where asking rents are currently more than \$10 per square foot less than asking rents in the area where the EPA Headquarters is currently located. Thus, the delineated area appears designed to limit competition, essentially guarantying that the lease transaction will not be on the most competitive terms available in downtown Denver.

GSA's solicitation requirement that offered buildings must be located within 1,320 walkable linear feet from a light rail station could also be interpreted as unduly restricting competition. In similar procurements, GSA has used a 2,640 foot radius to a light rail statements. Cutting GSA's standard radius by one-half, together with limiting public transportation requirement to light rail only, also appears to unduly restrict competition.

We are concerned that GSA is restricting competition through the delineated area requirement and the light rail requirement, and has rejected common-sense solutions to assist GSA in meeting its obligations and publicly stated policy goal of increasing competition. As a result, GSA is pursuing a sole-source lease.


We request that you review the solicitation process undertaken to date by GSA in connection with this procurement, and explain why GSA has acted contrary to administration and congressional policy in this lease procurement. We urge you to suspend any award of the replacement lease until you have addressed each of the concerns outlined in this letter.

Thank you for your attention to this matter.



PETER DeFAZIO
Ranking Member

Sincerely,



ANDRE CARSON
Ranking Member
Subcommittee on Economic
Development, Public Buildings, and
Emergency Management



November 22, 2016

The Honorable Jason Chaffetz
Chairman, Committee on Oversight
and Government Reform
House of Representatives
Washington, D.C. 20515

Dear Chairman Chaffetz:

Thank you for your letter to Administrator Denise Turner Roth dated October 20, 2016, regarding the U.S. General Services Administration's (GSA's) processes surrounding vehicle safety recalls. Your inquiry has been referred to me for response. GSA strongly believes in the importance of vehicle safety and that critical safety issues, including those identified in recall notices, should be promptly addressed.

GSA has two offices involved with Federal vehicle management. GSA's Office of Fleet Management (GSA Fleet) provides over 204,000 vehicles and efficient and economical fleet management services to over 75 participating Federal agencies. GSA Fleet is a mandatory source for vehicle purchases and an optional source for vehicle leasing. The other program involved is GSA's Office of Personal Property Management (GSA PPM), which disposes of approximately 7,000 vehicles per fiscal year on behalf of other Federal agencies. Per the Federal Management Regulation (FMR), GSA PPM is a mandatory source for disposal, via transfer or donation; however there are multiple approved Sales Centers. Because GSA does not manage the day-to-day operation of the vehicles that it leases to or disposes for other Federal agencies, providing recall information in a timely and practicable manner is essential to ensuring that vehicle recalls can be addressed by our partner Federal agencies.

GSA Fleet ensures that Federal drivers are notified of open, actionable recalls as soon as possible and provides customer leasing agencies with the tools and resources needed to actively manage recalls. For recalls that remain open, GSA sends monthly reminders to our customer agencies. Since GSA's automated vehicle recall process was implemented in 2012, GSA Fleet, with help from customer leasing agencies, has addressed and closed over 128,550 vehicle safety recalls.

GSA recently made improvements to its systems and processes to better track safety recalls to help ensure that they are promptly addressed. In July 2016, GSA Fleet made several enhancements to its GSA Fleet Drive-thru online customer portal. One of these improvements increased the visibility of recalls to customer leasing agencies by placing specific "flags" on affected vehicles when a customer reports preventative maintenance and/or mileage.

Recall information is also included in inventory reports that customers can run at-will or on a recurring basis. In addition, on October 1, 2016, GSA automated its electronic recall notifications to the customer contacts for affected vehicles. This enhancement allows for new notifications to be automatically sent the first of every month along with recurring reminders about recalls that remain open. Finally, on October 26, 2016, GSA Fleet met with the Motor Vehicle Executive Council, comprised of the Federal Fleet Managers, to discuss the recall issue and to identify ways to ensure a higher rate of compliance for closing safety recalls. GSA expects actionable steps to be developed to increase safety recall closure rates.

With respect to selling Federal vehicles to the public, GSA shares your concerns about providing full, accurate, and transparent information about vehicle recalls to potential purchasers. GSA Fleet's current practices require every prospective bidder to sign a registration form that contains terms and conditions with a disclaimer that vehicles may have open recalls. Those terms and conditions caution prospective bidders to verify a vehicle's recall status using either the manufacturer's or National Highway Traffic Safety Administration's (NHTSA) safercar.gov websites. Additionally, sales contracting officers are instructed to make an announcement at the beginning of each sale that any vehicle may have an open recall. During Fiscal Year 2016, GSA Fleet sold 37,486 vehicles, of which 98 percent of the vehicles sold did not have any actionable, open safety recalls.

When GSA's Personal Property Management Program sells other Federal agencies' vehicles, agencies are required to provide the property-related information outlined in 41 CFR § 102-36.235(b)(2) (FMR § 102-36.235(b)(2)), which states that "[i]f repairs are needed, the type of repairs" must be reported when applicable. Thus, Federal agencies must report any known repairs required when reporting property to PPM. If the owning agency provides outstanding recall information, GSA includes that information in the item description and/or with the attached documents for prospective bidders to review in GSA Auctions.

GSA's Fleet Program is exploring several options to improve recall closure rates:

1. GSA Fleet is looking at launching a new mobile fleet application, GSAFleet2Go, which would push recall notifications directly to customers' mobile devices. If actionable recalls are open on vehicles loaded to the customer's profile, a message about the recall will push to the mobile device. Customers could also check the Vehicle Reminders module in GSAFleet2Go for actionable recalls.
2. GSA Fleet is considering providing additional training to customers on how to use the new features in GSA Fleet Drive-thru that allow customer agencies access to recall data on their leased vehicles.

3. GSA Fleet will explore incorporating an automated data feed from a third-party that will provide data on all light duty vehicles regardless of the manufacturer. If successfully procured, that data will be more detailed than what is currently received - to include the NHTSA recall number and remedy status.
4. GSA Fleet will analyze how to best identify vehicles for sale with open safety recalls, and indicate this information on a vehicle-specific basis on GSA Fleet's website and in the sales catalog for each auction.
5. GSA Fleet will explore the possibility of adding recall notification data for vehicles owned by other Federal agencies that are included in GSA's Federal Fleet Management System (FedFMS). GSA offers FedFMS to Federal agencies at no additional cost to assist in the management of their Federal, agency-owned vehicles.
6. GSA Fleet is also exploring the feasibility of repairing vehicles with actionable safety recalls before sale and identifying the processes, procedures, systems enhancements, and resources that would be needed to implement any changes.

GSA's PPM program is examining improvements to its disposal of agency-owned vehicles:

1. GSA's PPM is looking into requiring all sales office managers to check for recalls on the NHTSA website prior to offering non-GSA-owned vehicles for sale on the GSA Auctions internet sales website. If a non-GSA-owned vehicle is subject to a recall, the GSA Sales Contracting Officer would disclose that information in the item description of the sale.
2. GSA's PPM, along with GSA's Office of Governmentwide Policy (OGP), is exploring how to highlight the importance of Federal agencies' disclosure of recall information for excess vehicles. OGP is looking into strengthening the language required by FMR § 102-36.235(b)(2) regarding vehicle item descriptions when agencies report excess vehicles to GSA. Enhanced FMR language, would allow PPM to make changes to the GSAXcess property reporting system to help remind Federal agencies of their reporting responsibilities.
3. GSA's PPM will assess providing more conspicuous indicators for vehicles with open recalls sold on the GSA Auctions internet website. GSA's PPM will also explore other ways to provide information about vehicle recalls to those interested in purchasing Government vehicles.

GSA will continue to strive to ensure that safe, reliable, cost-saving vehicle solutions are provided to assist Federal agencies in successfully meeting their missions. GSA shares your concerns regarding vehicle safety and appreciates your support of its concerted efforts to drive continuous improvements in the Federal fleet. The requested documents have been provided to your staff on a USB drive addressing the six questions identified in your inquiry.

If you have additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,



Lisa A. Austin
Associate Administrator

Enclosure

cc: The Honorable Elijah E. Cumming, Ranking Member, Committee on Oversight and Government Reform, House of Representatives
The Honorable Mark Meadows, Chairman Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives
The Honorable Gerald E. Connolly, Ranking Member, Subcommittee on Government Operations, Committee on Oversight and Government Reform, House of Representatives

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

October 20, 2016

The Honorable Denise Turner Roth
Administrator
General Services Administration
1800 F Street NW
Washington, D.C. 20405

Dear Administrator Roth:

We are writing to request your assistance in ensuring that vehicles used by federal employees are safe to drive and to seek your views on proposals to address federal vehicles sold or auctioned to the public that are subject to safety recalls.

Recent media reports have highlighted the issue of vehicle safety recalls. For example, one recent article described in detail how the Japanese company Takata has expanded recalls over the past several years to more than 60 million airbags in more than a dozen makes and models of vehicles after shrapnel from the devices killed ten people in the United States and injured many more.¹

We have a number of questions and concerns about vehicles in the federal fleet that are subject to these and other types of safety recalls.

First, we believe that no federal employees should be driving vehicles that are subject to recalls that could place employees or others at risk. One recent press account, however, has identified evidence suggesting that some vehicles with safety recalls have continued to be driven with open recalls. It stated:

Service tags on some of the vehicles Circa viewed indicate they had been driven months and sometimes years after the recall notices had been issued. That put federal employees who were behind the wheel before the cars were retired at potential risk. ...

The GSA wouldn't answer specific questions about cars with open recalls being driven by federal government employees. They said sometimes the recall notices go out after a fleet vehicle has been retired.

¹ Susan Berfield, et al., *Sixty Million Car Bombs: Inside Takata's Air Bag Crisis*, BLOOMBERG, June 2, 2016, available at <http://www.bloomberg.com/news/features/2016-06-02/sixty-million-car-bombs-inside-takata-s-air-bag-crisis>.

But we found cars used by agencies, including the United States Park Police and the Army, had been driven long after their recalls were issued.²

For these reasons, we would like to know what processes and procedures are used to ensure that no federal employees are driving vehicles that are subject to recalls that could affect their safety.

Second, we believe that no federal vehicles should be sold or auctioned to the public without clearly disclosing whether they are subject to open safety recalls. According to one recent press account, however, it is unclear whether this is currently being done:

GSA officials wouldn't talk on-camera, but said in a statement:

"The agency notifies all auction bidders and successful buyers in advance that there may be outstanding recalls on the sale vehicle, and to contact either their local dealership or use the NHTSA website to check the vehicle's recall status."

That notice is a small warning in print and a brief mention at the auction.³

Based on this information, it is unclear whether purchasers of federal vehicles are directly informed of open safety recalls, or instead are directed to other sources to determine whether this information exists. We understand that a new website was recently established for consumers to determine whether their vehicles are subject to open safety recalls.⁴ However, based on this information, it does not appear that federal agencies selling vehicles are currently required to disclose open safety recalls before the sales occur.

Third, we request your agency's views on requiring that all federal vehicles subject to open safety recalls be repaired before they are sold or auctioned to the public. Such action would appear to be consistent with the position of Mark Rosekind, the new Administrator of the National Highway Traffic Safety Administration, who stated: "We cannot allow vehicles with potentially dangerous defects to leave used-car lots without the necessary repairs."⁵

In order to address these questions, please provide the following documents and information by November 3, 2016:

1. A complete list of all GSA-owned vehicles subject to a safety recall, and the maintenance history of each vehicle since January 2014;

² Joce Sterman, et.al., *The Government Is Selling the Public Cars Without Repairing Safety Recall Defects*, CIRCA, Oct. 5, 2016, available at <http://circa.com/politics/accountability/feds-auction-off-hundreds-of-cars-with-unrepaired-recalls-possibly-putting-buyers-at-risk>.

³ *Id.*

⁴ *Keeping You Safe*, National Highway and Transportation Administration (online at www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues) (accessed Oct. 12, 2016).

⁵ *Used Cars Often Sold With Unfixed Defects, Despite Recalls*, ASSOC. PRESS, Feb. 24, 2015, available at http://www.oregonlive.com/business/index.ssf/2015/02/used_cars_often_sold_with_unfi.html.

October 20, 2016

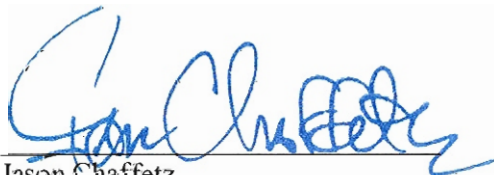
Page 3

2. A complete list of all GSA-owned vehicles sold at auction or transferred through the GSAXcess platform by VIN since January 2014;
3. A representative sample of the universe of documents provided to the public prior to or during a GSA vehicle auction, including, but not limited to, vehicle history disclosure forms, assumption of liability forms, and sales contracts;
4. All documents and communications referring or relating to the sale at auction, or transference through GSAXcess platform, of vehicles with open recalls;
5. Copies of GSA's vehicle recall and repair practices and procedures, including, but not limited to, a sample of letters used to notify agency lessees of open recalls and GSA's process for ensuring lessees repair known recalls; and
6. GSA's views on the feasibility of requiring that all federal vehicles subject to open safety recalls be repaired before they are sold or auctioned to the public.

When producing documents to the Committee, please deliver production sets to the Majority staff in room 2157 of the Rayburn House Office Building and the Minority staff in room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment to this letter provides additional information about responding to the Committee's request.

The Committee on Oversight and Government Reform is the principal investigative committee in the U.S. House of Representatives. Pursuant to House Rule X, the Committee has authority to investigate "any matter" at "any time."

Please contact Patrick Hartobey or Kevin Ortiz of the Majority staff at (202) 225-5074 or Lucinda Lessley of the Minority staff at (202) 225-5051 with any questions about this request. Thank you for your attention to this matter.

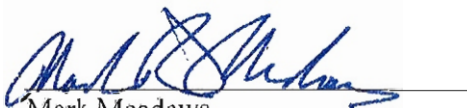


Jason Chaffetz
Chairman

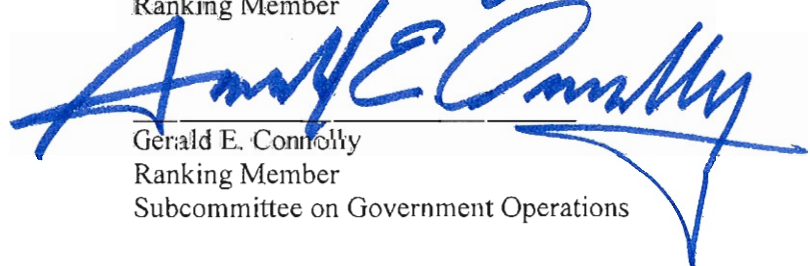
Sincerely,



Elijah E. Cummings
Ranking Member



Mark Meadows
Chairman
Subcommittee on Government Operations



Gerald E. Connolly
Ranking Member
Subcommittee on Government Operations

Enclosure

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
 - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
 - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,
CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE,
DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,
INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.
6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.
17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.

19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.
3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term “referring or relating,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term “employee” means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

February 8, 2017

The Honorable Saul Japson
Acting Associate Administrator
General Services Administration
1800 F Street, NW
Washington, D.C. 20405

Dear Administrator Japson:

Thank you for your letter on February 6, 2017, responding to our January 23, 2017, request for information regarding how the General Services Administration (GSA) is addressing President Donald Trump's apparent breach of the Old Post Office lease agreement.

We are writing pursuant to the statutory "Seven Member Rule" to obtain unredacted, complete copies of documents requested by our January 23, 2017 letter.

The Seven Member Rule is unique authority passed by Congress and signed by the President in 1928 that requires any executive agency to "submit any information requested of it relating to any matter within the jurisdiction of the committee" when requested by seven members of the Committee on Oversight and Government Reform.¹ Previously, 11 members of this Committee sent GSA a request pursuant to the Seven Member Rule on December 22, 2016, and GSA produced documents responsive to that request on January 3, 2017.²

Under House Rule X, the Committee has jurisdiction over "Government management and accounting measures generally," as well as the "Overall economy, efficiency, and management of government operations and activities, including Federal procurement."³ In addition, as the primary investigative body in the House, the Committee also has the broad authority "at any time to conduct investigations" of "any matter."⁴

¹ 5 U.S.C. § 2954. 45 Stat. 996 (1928). The statutory language originally referred to the "Committee on Government Operations." The Committee was renamed several times since then and in the 110th Congress, it was renamed the Committee on Oversight and Government Reform. References in law to the Committee on Government Operations are treated as referring to this Committee.

² Letter from Lisa A. Austin, Associate Administrator, to Ranking Member Elijah E. Cummings (Jan. 3, 2017).

³ House rule X, clause (1)(n).

⁴ House rule X, clause (4)(c)(2).

Pursuant to the Seven Member Rule, please provide the following documents no later than 5 p.m. on February 13, 2017:

1. Please provide, on an ongoing basis starting with November, monthly reports submitted to GSA by President Trump's company describing revenues and expenses.
2. Please provide copies of any correspondence from Trump Old Post Office LLC that provides notice of how it is addressing liens or documentation of any subsequent GSA action to resolve these liens.
3. Please provide copies of all correspondence with representatives of President Trump's company or the Trump transition team regarding the lease, the apparent breach of the lease, the monthly financial reports, the ownership structure of the Trump Old Post Office LLC, or any other matters above.
4. Please provide copies of the correspondence from Adam L. Rosen on December 16, 2016, and December 29, 2016, to GSA, referenced in the attachment to GSA's February 6, 2017, letter.

Thank you for your prompt cooperation with this matter.

Sincerely,

Thijs F. Lamme

Steph S. Lipp

Elleann H. Norton

Brenda Laurence

Peter Welch

Ann E. Canby

Jamie Rashin

Wm. Lacy Clay

The Honorable Saul Japson

Page 3

cc: The Honorable Jason Chaffetz, Chairman



Bobbi Conde - H1E <roberta.conde@gsa.gov>

Fwd: Request for information on hiring freeze

1 message

Erin Mewhirter - S <erin.mewhirter@gsa.gov>
Reply-To: executive-secretariat@gsa.gov
To: Executive Secretariat <executive-secretariat@gsa.gov>
Cc: Larnell Exum - S <larnell.exum@gsa.gov>, Antoinette Reaves <toni.reaves@gsa.gov>

Mon, Mar 6, 2017 at 3:40 PM

ExecSec - please control this Cummings inquiry to OCIA. Thanks. Erin

----- Forwarded message -----

From: **Antoinette Reaves - S** <toni.reaves@gsa.gov>
Date: Mon, Mar 6, 2017 at 9:41 AM
Subject: Fwd: Request for information on hiring freeze
To: Saul Japson <saul.japson@gsa.gov>
Cc: Brennan Hart - A <brennan.hart@gsa.gov>, Larnell Exum - S <larnell.exum@gsa.gov>, Erin Mewhirter <erin.mewhirter@gsa.gov>

----- Forwarded message -----

From: **Gollin, Elizabeth** <Elizabeth.Gollin@mail.house.gov>
Date: Mon, Mar 6, 2017 at 9:39 AM
Subject: Request for information on hiring freeze
To: "gsacongressionalaffairs@gsa.gov" <gsacongressionalaffairs@gsa.gov>, "larnell.exum@gsa.gov" <larnell.exum@gsa.gov>
Cc: "Davis, Charles" <Charles.Davis@mail.house.gov>

Good morning -

My name is Elizabeth from the House Committee on Oversight and Government Reform's Minority staff. In order to gain more insight into President Trump's hiring freeze, we would appreciate your response to the following questions:

1. Does the hiring freeze apply to the GSA?
2. If so, what positions does it affect?

3. Has the GSA issued guidance or a memo that exempts certain positions from the hiring freeze?

a. If so, what positions are exempted?

b. How many or what percentage of positions are exempted?

c. Please provide us with a copy of the written guidance or memo.

4. How many employees are there in the GSA?

5. How many total vacancies are there currently in the GSA? What types of positions are vacant and what are their numbers?

6. What percentage of GSA employees are retirement eligible?

7. How many or what percentage of employees does the GSA expect to retire in the next year?

a. What positions or departments are they located in?

8. What impact does/will the hiring freeze have on the GSA?

a. What is the impact on customer service?

If you have any questions, please feel free to email me or my colleague, Christopher Davis, at Charles.Davis@mail.house.gov.

Sincerely,

Elizabeth Gollin

House Committee on Oversight and Government Reform

(202) 225-5051 | 2471 Rayburn House Office Building

Rep. Elijah E. Cummings, Ranking Member

--

Antoinette S. Reaves

Office of Congressional and Intergovernmental Affairs

Washington, DC 20405

Desk 202-501-1543

Cell (b) (6)

Fax 202-219-5742

Lost time can never be found!

"You don't stop laughing because you grow old, you grow old because you stop laughing!"

--

Erin Mewhirter

Director of Congressional Operations

Office of Congressional and Intergovernmental Affairs

U.S. General Services Administration

www.gsa.gov



March 22, 2017

The Honorable Jason Chaffetz
Chairman
Committee on Oversight
and Government Reform
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your letter dated March 8, 2017, to Acting Administrator Timothy O. Horne requesting information pertaining the U.S. General Services Administration's (GSA) compliance with Federal recordkeeping and government transparency laws with respect to Federal employees' use of technology. Your inquiry has been referred to me for response.

GSA takes seriously its responsibilities to comply with the Federal Records Act and the Freedom of Information Act. In response to your six questions, we provide the following information.

1. Identify any senior agency officials who have used an alias email account to conduct official business since January 1, 2016. Include the name of the official, the alias account, and other email accounts used by the official to conduct official business.

Enclosed is a spreadsheet responsive to this request. The second tab of the worksheet contains a legend defining the terms alias, shared account, and Google group.

Please note that GSA's Inspector General reported that Phaedra Chrousos, a former senior agency official, used a personal email account to conduct official business.

2. Identify all agency policies referring or relating to the use of non-official electronic messaging accounts, including email, text message, messaging applications, and social media platforms to conduct official business, including but not limited to archiving and recordkeeping procedures.

The enclosed CIO 2100.1J *IT Security Policy* prohibits an employee or contractor supporting GSA from creating or sending information using a non-official GSA electronic messaging account unless a copy of the message is sent to an official GSA electronic messaging account. GSA's Inspector General recently reported lapses in compliance with this policy, which GSA management is in the process of addressing.

GSA's *Social Media Policy*, CIO 2106.1, discusses the use of social media technologies to enhance communication, collaboration, and information exchange in support of GSA's mission.

- The associated *Social Media Guide* provides applicable mandates and details on social media usage, and delineates the difference between "official capacity" and "personal capacity" so employees understand when they are posting for official business or acting on their own time and representing themselves.
- The Guide also addresses the practice of proper records management with regards to social media use.

The directive covering the *GSA Records Management Program*, OAS P 1820.1, states that any document that contains information required to transact the official business of GSA is a record (Page B-1). It also says that employees must take care to keep personal files separate from agency records, or in the event that a personal file contains agency records material, extract the official information and place it in an agency record file.

3. Identify all agency policies referring or relating to the use of official text message or other messaging or communications applications, and social media platforms to conduct official business, including but not limited to archiving and recordkeeping procedures.

The following GSA policies refer or relate to the use of official messaging or communication applications, and/or social media platforms to conduct official business.

GSA's *Social Media Policy*, CIO 2106.1, discusses the use of social media technologies to enhance communication, collaboration, and information exchange in support of GSA's mission.

- The associated *Social Media Guide* offers additional details on employee responsibilities when posting to social media.
- The Guide also addresses the practice of proper records management with regards to social media use.

- A narrative version provides an explanation of the policy and social media guide, the Social Media Navigator, on the GSA.gov site. It was recently updated to more thoroughly address recordkeeping and archiving responsibilities.

CIO 2160.2B *GSA Electronic Messaging and Related Services* provides direction on email and collaboration tools and additional requirements for managing electronic mail records.

OAS 1820.1 *GSA Records Management Program* defines what a Federal record is and details how all GSA records are to be handled and preserved as Federal records. GSA employees are required to maintain and preserve adequate records. The directive makes clear that records may exist in email, shared drives, GSA's Salesforce platform for sharing, the cloud, the chat function within Gmail, file cabinets, and desks.

4. Identify agency policies and procedures currently in place to ensure all communications related to the creation or transmission of Federal records on official electronic messaging accounts other than email, including social networking platforms, internal agency instant messaging systems and other communications applications, are properly captured and preserved as Federal records.

GSA has the following policies in place to ensure that all communications related to the creation or transmission of Federal records on official electronic messaging accounts – including email, social networking platforms, internal agency instant messaging systems and other communications applications – are properly captured and preserved as Federal records.

OAS 1820.1 *GSA Records Management Program* details how all GSA records are to be handled and preserved as Federal records and maintained in accordance with GSA's recordkeeping requirements.

GSA's *Social Media Policy*, CIO 2106.1, and associated Social Media Guide remind staff of the need to practice proper records management concerning social media.

In addition to formal policy directives, mandatory training for GSA employees includes guidance and procedures for dealing with records within electronic communications. GSA's records management training specifically refers to GSA's Salesforce application, "Chatter," text and chat applications (Google Chat, Skype, MMS and SMS services, and iMessage), Social Media applications, and generally to all "electronic messages" per 44 U.S.C. 2911.

5. Explain how your agency complies with FOIA requests that may require searching and production of documents stored on non-official email accounts, social networking platforms, or other messaging or communications.

The operation of GSA's FOIA Program is documented in the GSA Agency Annual Reports and the GSA Chief FOIA Officer's Reports that are posted annually on the GSA website (<https://www.gsa.gov/portal/content/129970>). Complete agency FOIA logs are also available on this site.

GSA complies with the FOIA Act in all respects and has policies and procedures in place for searching for the requested information. All requests are handled so as to fully comply with the law regardless of the nature of the request. As FOIA requests come into the agency, the GSA FOIA Division identifies the program or business line most likely to be responsible for the requested records. A Subject Matter Expert (SME) then assists in gathering potentially responsive information. The SME is responsible for searching for and examining relevant records, proposing redactions, and ensuring that all potentially responsive agency records are gathered for review and release to the FOIA requester.

In addition, the FOIA office will request that GSA IT conduct searches of all electronic databases for the requested information. The GSA Records Management Policy, OAS P 1820.1, provides that GSA employees maintain adequate records and that "records can exist in email, Chatter, share drives, Google drive, chat within Gmail, file cabinets, and/or desks" (OAS P 1820.1, page 8). "Chatter" is GSA's internal social media platform. Employees must ensure that "GSA business-related Internet and intranet postings, such as social media postings, Chatter postings, and collaborative worksite postings containing records are maintained in accordance with GSA's recordkeeping requirements" (OAS P 1820.1, page 2). Compliance with this policy ensures that GSA can access and retrieve any potentially releasable records for FOIA requests, regardless of electronic format.

6. Provide the status of compliance by the agency with the Managing Government Records Directive issued by the Office of Management and Budget on August 24, 2012.

GSA is in compliance with the Managing Government Records Directive issued by the Office of Management and Budget on August 24, 2012. The following details GSA's status on each goal outlined in the Directive:

- Goal 1.1 - By 2019, Federal agencies will manage all permanent electronic records in an electronic format.

GSA is in the process of rolling out a new electronic document management system (EDMS) that, when completed, will allow GSA to manage all permanent

electronic records electronically. This effort is on schedule to be completed by the 2019 deadline.

- Goal 1.2 - By 2016, Federal agencies will manage both permanent and temporary email records in an accessible electronic format.

GSA's Office of Administrative Services and GSA IT worked together during the past 2 years to implement the Capstone approach for agency email. GSA has a technical solution in place (Google Vault) to capture all agency email (other than that of the Office of Inspector General).

Currently, GSA is awaiting approval from the National Archives and Records Administration (NARA) of GSA's email retention schedule. Once this retention schedule is approved, GSA will formally issue a directive that addresses the disposition of email records.

- Goal 2.1 - Agencies must designate a Senior Agency Official (SAO).

GSA designated the Chief Administrative Services Officer as its Senior Agency Official.

- Goal 2.2 - SAO shall ensure that permanent records are identified for transfer and reported to NARA.

GSA has identified all permanent records that have existed for more than 30 years and reported them to NARA.

- Goal 2.3 - Agency records officers must obtain a NARA Certificate of Federal Records Management Training.

GSA's Agency Records Officer has a NARA Certificate of Federal Records Management Training.

- Goal 2.4 - Agencies must establish records management training.

GSA established mandatory records management training for all employees. This training is accessible through GSA's Online University.

- Goal 2.5 - SAO shall ensure that records are scheduled.

GSA has worked closely with NARA to create a records schedule that includes all agency record types. That schedule has been submitted to NARA for final approval.

An identical letter has been sent to your colleague. If you have any additional questions or concerns, please contact me at (202) 501-0563.

We appreciate your interest in GSA and records management.

Sincerely,

A handwritten signature in black ink, appearing to read "Saul Japson". The signature is stylized with a large, looped "S" and a trailing "y".

Saul Japson
Acting Associate Administrator

Enclosures



March 22, 2017

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight
and Government Reform
House of Representatives
Washington, DC 20515

Dear Representative Cummings:

Thank you for your letter dated March 8, 2017, to Acting Administrator Timothy O. Horne requesting information pertaining the U.S. General Services Administration's (GSA) compliance with Federal recordkeeping and government transparency laws with respect to Federal employees' use of technology. Your inquiry has been referred to me for response.

GSA takes seriously its responsibilities to comply with the Federal Records Act and the Freedom of Information Act. In response to your six questions, we provide the following information.

1. Identify any senior agency officials who have used an alias email account to conduct official business since January 1, 2016. Include the name of the official, the alias account, and other email accounts used by the official to conduct official business.

Enclosed is a spreadsheet responsive to this request. The second tab of the worksheet contains a legend defining the terms alias, shared account, and Google group.

Please note that GSA's Inspector General reported that Phaedra Chrousos, a former senior agency official, used a personal email account to conduct official business.

2. Identify all agency policies referring or relating to the use of non-official electronic messaging accounts, including email, text message, messaging applications, and social media platforms to conduct official business, including but not limited to archiving and recordkeeping procedures.

The enclosed CIO 2100.1J *IT Security Policy* prohibits an employee or contractor supporting GSA from creating or sending information using a non-official GSA electronic messaging account unless a copy of the message is sent to an official GSA electronic messaging account. GSA's Inspector General recently reported lapses in compliance with this policy, which GSA management is in the process of addressing.

GSA's *Social Media Policy*, CIO 2106.1, discusses the use of social media technologies to enhance communication, collaboration, and information exchange in support of GSA's mission.

- The associated *Social Media Guide* provides applicable mandates and details on social media usage, and delineates the difference between "official capacity" and "personal capacity" so employees understand when they are posting for official business or acting on their own time and representing themselves.
- The Guide also addresses the practice of proper records management with regards to social media use.

The directive covering the *GSA Records Management Program*, OAS P 1820.1, states that any document that contains information required to transact the official business of GSA is a record (Page B-1). It also says that employees must take care to keep personal files separate from agency records, or in the event that a personal file contains agency records material, extract the official information and place it in an agency record file.

3. Identify all agency policies referring or relating to the use of official text message or other messaging or communications applications, and social media platforms to conduct official business, including but not limited to archiving and recordkeeping procedures.

The following GSA policies refer or relate to the use of official messaging or communication applications, and/or social media platforms to conduct official business.

GSA's *Social Media Policy*, CIO 2106.1, discusses the use of social media technologies to enhance communication, collaboration, and information exchange in support of GSA's mission.

- The associated *Social Media Guide* offers additional details on employee responsibilities when posting to social media.
- The Guide also addresses the practice of proper records management with regards to social media use.

- A narrative version provides an explanation of the policy and social media guide, the Social Media Navigator, on the GSA.gov site. It was recently updated to more thoroughly address recordkeeping and archiving responsibilities.

CIO 2160.2B *GSA Electronic Messaging and Related Services* provides direction on email and collaboration tools and additional requirements for managing electronic mail records.

OAS 1820.1 *GSA Records Management Program* defines what a Federal record is and details how all GSA records are to be handled and preserved as Federal records. GSA employees are required to maintain and preserve adequate records. The directive makes clear that records may exist in email, shared drives, GSA's Salesforce platform for sharing, the cloud, the chat function within Gmail, file cabinets, and desks.

4. Identify agency policies and procedures currently in place to ensure all communications related to the creation or transmission of Federal records on official electronic messaging accounts other than email, including social networking platforms, internal agency instant messaging systems and other communications applications, are properly captured and preserved as Federal records.

GSA has the following policies in place to ensure that all communications related to the creation or transmission of Federal records on official electronic messaging accounts – including email, social networking platforms, internal agency instant messaging systems and other communications applications – are properly captured and preserved as Federal records.

OAS 1820.1 *GSA Records Management Program* details how all GSA records are to be handled and preserved as Federal records and maintained in accordance with GSA's recordkeeping requirements.

GSA's *Social Media Policy*, CIO 2106.1, and associated Social Media Guide remind staff of the need to practice proper records management concerning social media.

In addition to formal policy directives, mandatory training for GSA employees includes guidance and procedures for dealing with records within electronic communications. GSA's records management training specifically refers to GSA's Salesforce application, "Chatter," text and chat applications (Google Chat, Skype, MMS and SMS services, and iMessage), Social Media applications, and generally to all "electronic messages" per 44 U.S.C. 2911.

5. Explain how your agency complies with FOIA requests that may require searching and production of documents stored on non-official email accounts, social networking platforms, or other messaging or communications.

The operation of GSA's FOIA Program is documented in the GSA Agency Annual Reports and the GSA Chief FOIA Officer's Reports that are posted annually on the GSA website (<https://www.gsa.gov/portal/content/129970>). Complete agency FOIA logs are also available on this site.

GSA complies with the FOIA Act in all respects and has policies and procedures in place for searching for the requested information. All requests are handled so as to fully comply with the law regardless of the nature of the request. As FOIA requests come into the agency, the GSA FOIA Division identifies the program or business line most likely to be responsible for the requested records. A Subject Matter Expert (SME) then assists in gathering potentially responsive information. The SME is responsible for searching for and examining relevant records, proposing redactions, and ensuring that all potentially responsive agency records are gathered for review and release to the FOIA requester.

In addition, the FOIA office will request that GSA IT conduct searches of all electronic databases for the requested information. The GSA Records Management Policy, OAS P 1820.1, provides that GSA employees maintain adequate records and that "records can exist in email, Chatter, share drives, Google drive, chat within Gmail, file cabinets, and/or desks" (OAS P 1820.1, page 8). "Chatter" is GSA's internal social media platform. Employees must ensure that "GSA business-related Internet and intranet postings, such as social media postings, Chatter postings, and collaborative worksite postings containing records are maintained in accordance with GSA's recordkeeping requirements" (OAS P 1820.1, page 2). Compliance with this policy ensures that GSA can access and retrieve any potentially releasable records for FOIA requests, regardless of electronic format.

6. Provide the status of compliance by the agency with the Managing Government Records Directive issued by the Office of Management and Budget on August 24, 2012.

GSA is in compliance with the Managing Government Records Directive issued by the Office of Management and Budget on August 24, 2012. The following details GSA's status on each goal outlined in the Directive:

- Goal 1.1 - By 2019, Federal agencies will manage all permanent electronic records in an electronic format.

GSA is in the process of rolling out a new electronic document management system (EDMS) that, when completed, will allow GSA to manage all permanent

electronic records electronically. This effort is on schedule to be completed by the 2019 deadline.

- Goal 1.2 - By 2016, Federal agencies will manage both permanent and temporary email records in an accessible electronic format.

GSA's Office of Administrative Services and GSA IT worked together during the past 2 years to implement the Capstone approach for agency email. GSA has a technical solution in place (Google Vault) to capture all agency email (other than that of the Office of Inspector General).

Currently, GSA is awaiting approval from the National Archives and Records Administration (NARA) of GSA's email retention schedule. Once this retention schedule is approved, GSA will formally issue a directive that addresses the disposition of email records.

- Goal 2.1 - Agencies must designate a Senior Agency Official (SAO).

GSA designated the Chief Administrative Services Officer as its Senior Agency Official.

- Goal 2.2 - SAO shall ensure that permanent records are identified for transfer and reported to NARA.

GSA has identified all permanent records that have existed for more than 30 years and reported them to NARA.

- Goal 2.3 - Agency records officers must obtain a NARA Certificate of Federal Records Management Training.

GSA's Agency Records Officer has a NARA Certificate of Federal Records Management Training.

- Goal 2.4 - Agencies must establish records management training.

GSA established mandatory records management training for all employees. This training is accessible through GSA's Online University.

- Goal 2.5 - SAO shall ensure that records are scheduled.

GSA has worked closely with NARA to create a records schedule that includes all agency record types. That schedule has been submitted to NARA for final approval.

An identical letter has been sent to your colleague. If you have any additional questions or concerns, please contact me at (202) 501-0563.

We appreciate your interest in GSA and records management.

Sincerely,

A handwritten signature in black ink, appearing to read "Saul Japson".

Saul Japson
Acting Associate Administrator

Enclosures

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2100.1J CHGE 1
April 28, 2016

GSA ORDER

SUBJECT: GSA Information Technology (IT) Security Policy

1. Purpose. This Order issues GSA's Information Technology Security Policy.
2. Cancellations.
 - a. [CIO P 2100.1I CHGE 1, GSA Information Technology \(IT\) Security Policy](#) is cancelled.
 - b. [CIO IL-14-02 Authority-to-Operate \(ATO\) Extensions/Limited ATO](#) is cancelled.
 - c. [CIO IL-13-01 Mobile Devices and Applications](#) is cancelled.
 - d. [CIO IL-15-02 Updated Policy Statements for Personally Identifiable Information \(PII\)](#) is cancelled.
3. Revisions. This Order provides updates for consistency with Federal requirements and program instruction implementation. Changes include:
 - a. Throughout document, changes were made to support CIO consolidation efforts.
 - b. Addition of Chapter 6: Privacy Controls.
 - c. Incorporates information from Instructional Letters: [CIO IL-14-02 Authority-to-Operate \(ATO\) Extensions/Limited ATO](#), [CIO IL-15-02 Updated Policy Statements for Personally Identifiable Information \(PII\)](#) and [CIO IL-14-04 Internal Clearance Process for GSA Data Assets](#) into the policy.
 - d. Includes information from new Directives: [CIO 2130.2 Enterprise IT Governance](#), [CIO 2105.1C CHGE 1 GSA Section 508: Managing Information and Communications Technology \(ICT\) for Individuals with Disabilities](#), and [MV-15-01 Contract Guidance on Information and Information Systems Security](#).
 - e. Includes new public law issued November 2014 – [Public Law No: 113-187](#) Section 10 –Presidential & Federal Records Act Amendments.

f. Incorporates requirements from [OAS P 1820.1 GSA Records Management Program](#).

4. Applicability. This IT Security Policy applies to all individuals or corporate entities that process or handle GSA-owned information, data, all GSA IT systems, or any GSA data processed on IT systems owned and operated by any of the Services or Staff Offices. Contracting Officers must include compliance with this policy in the contract or task order for contractor employees (see Chapter 1 Section 11). This policy applies to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act and it does not conflict with other OIG policies or the OIG mission.

5. Explanation of change paragraph. Chapter 2, Section 15(f) is amended to add the following highlighted:

“f. Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver, and removing PIV card before leaving their workstation.”

6. Signature.

/S/_____
DAVID SHIVE
Chief Information Officer
Office of GSA IT

Table of Contents

<u>CHAPTER 1: THE GSA INFORMATION TECHNOLOGY SECURITY PROGRAM</u>	1
1. Introduction.....	1
2. Objectives.....	1
3. Federal laws and regulation	2
4. GSA policies.....	3
5. Compliance and deviation/waivers	4
6. Maintenance.....	4
7. Definition of information system.....	4
8. NIST and GSA guidance documents.....	4
9. Privacy Act systems	5
10. IT security controls	5
11. Contractor operations	5
<u>CHAPTER 2: SECURITY ROLES AND RESPONSIBILITIES</u>	6
1. GSA Administrator.....	6
2. GSA Chief Information Officer (CIO)	6
3. GSA Chief Financial Officer (CFO).....	7
4. GSA Senior Agency Official for Privacy.....	8
5. GSA Chief Information Security Officer (CISO)	9
6. Heads of Services and Staff Offices (HSSOs).....	11
7. Authorizing Official (AO)	11
8. Office of CISO Division Directors.....	14
9. Information Systems Security Manager (ISSM).....	14
10. Information Systems Security Officer (ISSO).....	15
11. System Owners	17
12. Data Owners	20
13. Contracting Officers and Contracting Officer's Representatives.....	21
14. Custodians.....	22
15. Authorized Users of IT Resources.....	23
16. GSA Inspector General (IG)	24
17. GSA Personnel Security Officer/Office of Human Resources Management.....	26
18. System/Network Administrators.....	26
19. Supervisors.....	27
<u>CHAPTER 3: POLICY ON MANAGEMENT CONTROLS</u>	28
1. Management controls from control families	28
2. Policy on controls for the security management of GSA systems.....	28
<u>CHAPTER 4: POLICY ON OPERATIONAL CONTROLS</u>	35
1. Operational controls from control families	35
2. Policy on controls for the operational security of the system	35

[CHAPTER 5: POLICY ON TECHNICAL CONTROLS](#).....54

1. Technical controls from control families 54

2. Policy on controls for identification and authentication, access control,
auditing and others54

[CHAPTER 6: POLICY ON PRIVACY CONTROLS](#)64

1. Authority and purpose64

2. Accountability, audit, and risk management64

3. Data quality and integrity65

4. Data minimization and retention65

5. Individual participation and redress65

6. Use Limitation.....66

CHAPTER 1: THE GSA INFORMATION TECHNOLOGY SECURITY PROGRAM

1. Introduction. The purpose of this Order is to document and set forth the General Services Administration (GSA) Information Technology (IT) Security Policy. This IT Security Policy establishes controls required to comply with Federal regulations and laws, thus facilitates adequate protection of GSA IT resources.

2. Objectives. IT Security Policy objectives will enable GSA to meet its mission/business objectives by implementing systems with due consideration of IT-related risks to GSA, its partners, and customers. The security objectives for system resources are to provide assurance of confidentiality, integrity, availability, and accountability, by employing management, operational, and technical security controls as part of risk-based management. An important component of risk-based management is to integrate technical and non-technical security mechanisms into the system to reflect sound risk management practices. All incorporated security mechanisms must be well founded, configured to perform in the most effective manner, and add value to GSA's IT-related investments. A risk-based management approach will enable the GSA IT Security Program to meet its goals by better securing IT systems, enabling management to justify IT Security expenditures, and by assisting management in authorizing IT systems for processing. GSA IT Security objectives include the following:

a. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Private or confidential information is not disclosed to unauthorized individuals while in storage, during processing, or in transit.

b. Integrity. Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. Safeguards must ensure that information retains its content integrity. Hardware and software resources of the system must operate according to requirements and design documents. Un-authorized personnel must not be able to create, alter, copy, or delete data processed, stored, or handled by the system. System information and application software is considered "official" and accurate as the basis for business decisions.

c. Availability. Ensuring timely and reliable access to and use of information. The system works promptly and service is not denied to authorized users. Systems and data are available for intended use only. The system must be ready for use by authorized users when needed to perform his/her duties.

d. Accountability. Accountability must be to the individual level. Only personnel with proper authorization and need-to-know must be allowed access to data processed, handled, or stored on IT system components.

e. Assurance. Confidence that the other four security objectives have been met. The security measures, including: technical, managerial, and operational, work as intended to protect the system and the information it processes. This assurance is provided through monitoring and review of controls.

This Order supports GSA's IT Security Program objectives by identifying roles and assigning responsibilities in support of GSA's IT Security Program. In addition, the Order defines comprehensive and integrated security requirements that are necessary to obtain management authorization to allow GSA IT systems to operate within an acceptable level of security risk. The order also supports GSA's objective to ensure that all outsourced cloud services are from FedRAMP compliant cloud service providers, and leverage existing ATOs from other agencies to maximize savings. In addition to the security requirements in this Order, systems that contain payment card data or purchase/credit card numbers must implement the additional security controls known as security requirements as defined in Payment Card Industry Data Security Standard (PCI DSS) published by the PCI Security Standards Council as directed by the Financial Management Services of the Department of Treasury.

3. Federal laws and regulations. The primary focus of this policy is to provide guidelines that support the implementation of the following Federal regulations and laws, and the latest versions of the GSA directives in the next section:

- Federal Information Security Management Act ([FISMA](#)) of 2002.
- [Clinger-Cohen Act of 1996](#) also known as the Information Technology Management Reform Act (ITMRA) of 1996.
- Federal Financial Management Improvement Act of 1996 ([FFMIA](#)); OMB Implementation Guidance for the FFMIA.
- Paperwork Reduction Act ([PRA](#)) of 1995 (Public Law 104-13).
- Federal Managers Financial Integrity Act ([FMFIA](#)) (Public Law 97-255).
- Government Paperwork Elimination Act ([GPEA](#)) (Public Law 105-277).
- [Privacy Act](#) of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive ([HSPD-20](#)), National Continuity Policy.
- Homeland Security Presidential Directive ([HSPD-12](#)), Policy for a Common Identification Standard for Federal Employees and Contractors.
- Homeland Security Presidential Directive ([HSPD-7](#)), Critical Infrastructure Identification, Prioritization, and Protection.
- Office of Management and Budget (OMB) [Circular A-130](#), Management of Federal Information Resources, and Appendix III, Security of Federal Automated Information Systems as amended.
- Public Law No: 113-187, [Presidential and Federal Records Act Amendments of 2014, Section 10, Disclosure requirement for official business conducted using non-official electronic messaging account.](#)
- Open Data Policy -- Managing Information as an Asset [OMB Memorandum M-13-13](#).
- [Payment Card Industry Data Security Standard \(PCI DSS\)](#)

- [Executive Order 13556 Controlled Unclassified Information](#)

4. GSA policies:

- [GSA Order ADM 7800.11A](#), Personal Use of Agency Office Equipment
- [GSA Order ADM P 9732.1](#), Suitability and Personnel Security
- [GSA Order CIO 1878.1](#), GSA Privacy Act Program
- [GSA Order CIO 1878.2A](#), Conducting Privacy Impact Assessments (PIAs) in GSA
- [GSA Order CIO 2100.2B](#), GSA Wireless Local Area Network (LAN) Security
- [GSA Order CIO 2102.1](#), IT Information Technology (IT) Integration Policy
- [GSA Order CIO 2104.1A](#), GSA Information Technology (IT) General Rules of Behavior
- [GSA Order CIO 2110.2](#), GSA Enterprise Architecture Policy
- [GSA Order CIO 2135.2B](#), GSA Information Technology (IT) Capital Planning and Investment Control
- [GSA Order CIO 2140.3](#), Systems Development Life Cycle (SDLC) Policy
- [GSA Order CIO 2160.2B](#), GSA Electronic Messaging and Related Services
- [GSA Order CIO 9297.1](#), GSA Data Release Policy
- [GSA Order CIO 9297.2](#), GSA Information Breach Notification Policy
- [GSA Order CIO P 2165.2](#), GSA Telecommunications Policy
- [GSA Order CIO P 2180.1](#), GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- [GSA Order CIO P 2181.1](#), Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing
- [GSA Order CIO P 2182.2](#), Mandatory Use of Personal Identity Verification (PIV) Credentials
- [Bring Your Own Device](#): A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs, August 23, 2012
- [MV-15-01](#), Contract Guidance on Information and Information Systems Security (GSAM 552.239-71)
- [GSA Order CIO IL-15-02](#), Updated Policy Statements for Personally Identifiable Information (PII)
- [GSA Order OAS P 1820.1](#), GSA Records Management Program

Note:

- In addition to the principles set forth in GSA Order CIO 2110.2, architecture practices cited in OMB's The Common Approach to Federal Enterprise Architecture must be used during planning of a new system or significant capability enhancement.
- Executive Order 13556 implements the Controlled Unclassified Information (CUI) program. OCISO will provide additional guidance upon implementation of the program at GSA. Please contact the OCISO at itsecurity@gsa.gov or the CUI Program Manager at cui@gsa.gov for additional information.

- Additional policies, procedures and guidance can be found in the GSA IT Security InSite main page: <https://insite.staging.gsa.gov/portal/category/534722>. The guides provide more detailed information on how to implement security processes and controls and provide worksheets and forms to meet reporting requirements. The guides are updated as needed to reflect the latest regulations and technologies. A current list of Government-wide security guidance provided by the National Institute of Standards and Technology (NIST) is located at <http://csrc.nist.gov/publications/PubsSPs.html>.

5. Compliance and deviation/waivers. Compliance is mandatory immediately upon signing. This IT Security Policy requires all GSA Services, Staff Offices, Regions (S/SO/R), Federal employees, contractors and other authorized users of GSA's IT resources, to comply with the security requirements outlined in this policy. This policy must be properly implemented, enforced, and followed to effectively protect GSA's IT resources and data. Appropriate disciplinary actions must be taken in a timely manner in situations where individuals and/or systems are found non-compliant. Violations of this GSA IT Security Policy may result in penalties under criminal and civil statutes.

All deviations/waivers from this Order must be approved by the appropriate Authorizing Official with a copy of the approval forwarded to the GSA Chief Information Security Officer (CISO) in the Office of GSA IT for concurrence.

6. Maintenance. The GSA Office of the Chief Information Security Officer (OCISO) will review this policy at least annually and revise it to:

- Reflect any changes in Federal laws and regulations;
- Satisfy additional business requirements;
- Encompass new technology;
- Adopt new Government IT standards.

7. Definition of information system. The term *information system* as defined in this document shall include major applications and general support systems as defined in OMB A-130. Major Applications shall include those information systems with an Exhibit 300 (also referred to as Major Programs) and any Exhibit 53 information systems that are not specifically covered in a general support system security plan. In addition, any IT system that stores privacy act data that is not specifically covered in a general support system shall be considered its own information system.

Smaller information systems (minor applications) may be coalesced together as subsystems of a single larger, more comprehensive system for the purposes of security authorization. Subsystems must be under the same management authority, have the same function or mission objective, the same operating characteristics and information security needs, and reside in the same general operating environment(s).

8. National Institute of Standards and Technology (NIST) and GSA guidance documents. All policies shall be implemented using the appropriate special publications

from NIST and/or GSA procedural guides to the greatest extent possible. Where there is a conflict between NIST guidance and GSA guidance, contact the GSA Office of the Chief Information Security Officer. Where there are no procedural guides, use industry best practices. Federal Information Processing Standards (FIPS) publication requirements are mandatory for use at GSA.

NIST special publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory. Waivers for compliance to NIST special publications, (refer to 1.6 above for GSA deviations/waivers) must be based on an approved risk based decision that includes a date of resolution to comply.

9. Privacy Act systems. In addition to the security requirements in this Order, systems that contain privacy act data or personally identifiable information must implement the additional security controls as defined in [NIST SP 800-53](#), Appendix J: Privacy Control Catalog, GSA Order CPO 1878.1 Privacy Act Program under “Information Security” and GSA Order CIO 1878.2, CIO P Conducting Privacy Impact Assessments (PIA) in GSA.

10. IT security controls. All IT systems, including those operated by a contractor on behalf of the Government, must implement proper security controls according to the security categorization level in accordance with FIPS [Publication 200](#), Minimum Security Requirements for Federal Information and Information Systems, [FIPS PUB 199](#), Standards for Security Categorization of Federal Information and Information Systems, the current version of [NIST SP 800-53](#) R4, Security and Privacy Controls for Federal Information Systems and Organizations.

11. Contractor operations.

a. GSA system program managers and contracting officers shall ensure that the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on behalf of the Government, including systems operating in a Cloud Computing environment including but not limited to Software as a Service (SaaS) and Platform as a Service (PaaS). In addition, the Government shall ensure that the contract allows the Government or its designated representative (i.e. third party contractor) to review, monitor, test, and evaluate the proper implementation, operation, and maintenance of the security controls. This requirement includes, but is not limited to: documentation review, server configuration review, vulnerability scanning, code review, physical data center reviews, and operational process reviews and monitoring of SSAE 16 reporting control submissions.

b. The security controls implemented as part of contracts and task orders must also include specific language that requires solutions to align with existing Information Security architecture. Additional information may be found in IT Security Procedural Guide: Security Language for IT Acquisition Efforts, OCIO-IT Security-09-48.

CHAPTER 2: SECURITY ROLES AND RESPONSIBILITIES

The roles and responsibilities described in the paragraphs below are assigned to the offices and positions identified to ensure effective implementation and management of GSA's IT Security Program. The establishment of a security management structure and assigning of security responsibilities is a requirement of the Federal Information Security Management Act (FISMA).

1. GSA Administrator. The Clinger-Cohen Act assigns the responsibility for ensuring "that the information security policies, procedures, and practices of the executive agency are adequate." FISMA provides the following details on agency head responsibilities for information security:

a. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

b. Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization.

c. Ensuring that information security processes are integrated with strategic and operational planning processes to secure the organization's mission.

d. Ensuring that senior agency officials within the organization are given the necessary authority to secure the operations and assets under their control.

e. Designating a Chief Information Officer (CIO) and delegating authority to that individual to ensure compliance with applicable information security requirements.

f. Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines.

g. Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions.

2. GSA Chief Information Officer (CIO). Mandated by the Clinger-Cohen Act of 1996 and FISMA, the GSA CIO has overall responsibility for the GSA IT Security Program. Responsibilities include:

a. Developing and maintaining an agency-wide GSA IT Security Program.

- b. Ensuring the agency effectively implements and maintains information security policies and guidelines.
- c. Providing guidance, advice, and assistance to the Heads of Services and Staff Offices (HSSOs), and Regional Administrators (RAs) on implementing GSA's IT Security Policy.
- d. Providing management processes to enable the Authorizing Official to implement the components of the IT Security Program for which they are responsible.
- e. Ensuring information assurance and the protection of GSA's cyber-based critical infrastructure.
- f. Designating a Chief Information Security Officer (CISO) to assist in carrying out the GSA CIO's agency-wide IT security responsibilities.
- g. Establishing reporting requirements within GSA to assess GSA's IT security posture, verifying compliance with Federal requirements and approved policies, and identifying agency-wide IT security needs.
- h. Conducting independent activities and compliance reviews including oversight of GSA's Assessment and Authorization (A&A) process.
- i. Coordinating and reporting on HSPD-7 critical assets.
- j. Reporting annually, in coordination with the other senior agency officials, to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.
- k. Reviewing Privacy Impact Assessments prepared by GSA organizations for security considerations.
- l. Ensuring Privacy Impact Assessments are part of GSA's System Development Life Cycle Guidance for Information Technology.
- m. Providing guidance or input for periodic assessments of S/SO/R security measures and goals to assure implementation of GSA policy and procedures.

3. GSA Chief Financial Officer (CFO). The GSA Chief Financial Officer (CFO) also has major statutory security responsibilities under the CFO Act of 1990 and the [Clinger-Cohen Act of 1996](#). Responsibilities include:

- a. Developing and maintaining an integrated agency accounting and financial management system, including financial reporting and internal controls, which comply with FMFIA and FFMI requirements;

b. Complying with such policies and requirements as may be prescribed by the Director of the Office of Management and Budget (OMB);

c. Complying with applicable accounting principles, standards, and requirements, and internal control standards and any other requirements applicable to such systems;

d. Supporting the GSA IT Capital Planning Process. To achieve satisfactory assurance levels of information security for the financial systems of GSA, close cooperation between the offices of the CFO and the CIO is necessary, including supporting the GSA IT Capital Planning process;

e. Reporting financial management information to OMB as part of the President's budget;

(1) Complying with legislative and OMB-defined responsibilities as they relate to IT capital investments; and

(2) Ensuring that the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor that hosts GSA financial systems. This includes, but is not limited to: documentation review of operational processes and reviews that monitor SSAE 16 reporting submissions.

4. GSA Senior Agency Official for Privacy. GSA has identified the CIO as the Senior Agency Official for Privacy (SAOP) having major statutory responsibilities under the Privacy Act of 1974, [GSA Order CIO 1878.1](#), and the [Consolidated Appropriations Act of 2005](#). Responsibilities include:

a. Establishing and overseeing the Privacy Act Program in GSA.

b. Ensuring GSA's compliance with privacy laws, regulations and GSA policy.

c. Ensuring GSA's compliance with [NIST SP 800-53](#), Appendix J: Privacy Control Catalog.

d. Ensuring that GSA data assets go through secure clearance processing prior to public release and that applicable Privacy Policies are followed. The specific policy is detailed in Section 6.7 of this document.

e. Ensuring Privacy Impact Assessments (PIAs) are conducted for electronic information systems and collections and coordinating submission of all GSA Privacy Analysis Worksheets and PIA Summaries to OMB.

f. Developing, implementing, and overseeing personnel security controls for access to personally identifiable information.

- g. Encouraging awareness of potential privacy issues and policies.
- h. Directing the planning and implementation of the GSA Privacy Program to ensure agency personnel, including contractors, receive appropriate privacy awareness training to include IT Security and Privacy Awareness annual training, Privacy 201 training and Sharing Information in a Collaborative Environment training.
- i. Signing GSA Privacy Act notices for publication for public comment in the Federal Register.
- j. Reporting to OMB and Congress on the establishment or revision of Privacy Act systems.
- k. Reporting periodically to OMB on GSA Privacy Act activities, as required by law and OMB information requests.
- l. Policy making role in GSA's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues.
- m. Chairing the GSA Data Integrity Board that reviews and approves GSA's Computer Matching Program.

5. GSA Chief Information Security Officer (CISO) (formerly known as Senior Agency Information Security Officer). The Federal Information Security Management Act (FISMA) establishes the designation of a Senior Agency Information Security Officer. GSA has assigned that responsibility to the Chief Information Security Officer (CISO). The CISO is the focal point for all GSA IT security and must ensure that the security requirements described in this Order are implemented agency-wide. The CISO reports directly to the CIO as required by FISMA. Responsibilities include:

- a. Reporting to the GSA CIO on the implementation and maintenance of the GSA's IT Security Program and Security Policies.
- b. Assisting in the oversight of GSA's IT Security Program and Security Policies.
- c. Reporting to the GSA CIO on activities and trends that may affect the security of systems and applications assigned to GSA.
- d. Implementing and overseeing GSA's IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with this policy.
- e. Ensuring that written agreements assign security-related functions and identify security responsibilities of each S/SO/R or activity when two or more activities use the same IT.
- f. Providing guidance and advice to all S/SO/R on IT security issues.

g. Assisting S/SO/R in implementing the IT Security Program and Security Policies when requested.

h. Reporting to agency senior management on policy compliance.

i. Directing the planning and implementation of the GSA IT Security Awareness and Privacy Training Program to ensure agency personnel, including contractors, receive appropriate security and privacy awareness training including "Sharing Information in a Collaborative Environment" training.

j. Managing the CIO Office of the CISO which implements the GSA IT Security and Privacy Programs.

k. Establishing reporting deadlines for IT Security related issues requiring an agency response affecting the GSA IT Security Program.

l. Performing information security duties as the primary duty.

m. Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

n. Periodically testing and evaluating the effectiveness of information security policies, procedures, and practices.

o. Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.

p. Developing and implementing procedures for detecting, reporting, and responding to security incidents.

q. Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of GSA.

r. Supporting the GSA CIO in annual reporting to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.

s. Developing and implementing IT security performance metrics to evaluate the effectiveness of technical and nontechnical safeguards used to protect GSA information and information systems.

- t. Assessing S/SO/R security measures and goals periodically to assure implementation of GSA policy and procedures.
- u. Ensuring the appointment in writing of the ISSM and ISSOs for each system.
- v. Administering FISMA requirements and coordinating GSA's annual FISMA security program review and Plan of Action and Milestones (POA&M) implementations.
- w. Ensuring that the ISSMs and ISSOs receive applicable security and privacy awareness training to carry out their duties.
- x. Ensuring that IT Acquisitions align with GSA Information Security requirements.

6. Heads of Services and Staff Offices (HSSOs). HSSOs are responsible for authorizing the operation of all systems, networks, and applications for which they have responsibility. They may delegate some of their authority, (i.e., the role of Authorizing Official in writing), to appropriately qualified individuals within their organizations. Responsibilities include:

- a. Ensuring adherence and proper implementation of GSA's IT Security Policy.
- b. Ensuring that the systems of record under their jurisdiction meet the requirements of the Privacy Act and GSA privacy policies and procedures.
- c. Ensuring that contractors performing services associated with systems of record (such as system development, maintenance, or operation) are subject to the provisions of the Privacy Act and security requirements.
- d. Tracking the measures and goals described in Chapter 3 (i) Performance Measures of this policy and ensuring that AOs, ISSMs, and ISSOs support these measures.
- e. Ensuring System Owners adhere to the GSA Records Management Program.

7. Authorizing Official (AO). The Authorizing Official (AO) is the Federal Government management official with the responsibility to identify the level of acceptable risk for an IT system or application and to determine whether the acceptable level of risk has been obtained. Final authority to operate or not operate the system rests with the AO. An AO must be assigned to every information system. An AO may have responsibility for more than one system, provided there is no conflict. Responsibilities include:

- a. Ensuring adherence to GSA's IT Security Policy.
- b. Reviewing and approving security safeguards of information systems and issuing accreditation statements for each information system under their jurisdiction based on the acceptability of the security safeguards of the system (risk-management approach).

c. Ensuring that an Interim Authorization to Operate (IATO) is granted only if the necessary security enhancements to bring the system to the acceptable level of risk have been identified and a formal plan of action and milestones has been developed. Information systems with an expiring ATO may perform a one-time extension of the current authorization for a period not to exceed one year (365 days) from the date of ATO expiry to allow development of near real-time continuous monitoring capabilities to support ongoing authorization.

d. Ensuring that GSA systems that are planned to be decommissioned may request a one-time ATO extension for a period not to exceed one year (365 days) from the date of the ATO expiry.

e. Ensuring that GSA information systems that are planned to be consolidated into another system or transitioned into a cloud environment may request an ATO extension, for a period not to exceed one year (365 days), to allow the information system to receive an ATO as part of the consolidated information system or its new cloud environment of operation. The scope of consolidation and/or the change in the system environment shall be approved by Office of the Chief Information Security Officer (OCISO) prior to submitting the ATO extension request for the system.

f. Ensuring that GSA information systems that have undergone a full security assessment of all NIST SP 800-53 controls at the appropriate FIPS 199 impact level as part of a three-year re-authorization, and have outstanding high and critical vulnerabilities identified as part of security assessment, may request a limited ATO extension for a period not to exceed 30 days from the date of the ATO expiry to allow mitigation of the high and critical vulnerabilities.

g. Ensure that new GSA information systems pursuing an agile development methodology and residing on infrastructures that have a GSA ATO concurred by the OCISO or a FedRAMP ATO may request a limited ATO for the pilot period of the project not to exceed one year (365 days). The limited ATO will be based on a lightweight security assessment and authorization (A&A) process; however, the period of the limited ATO should be used to conduct a full A&A resulting in a new three-year ATO.

h. Ensuring that under any and all circumstances, in which an ATO is issued for less than three years, the GSA system continues to perform monthly Operating System scans (with Root/Administrative privileges), Database scans (DBA privileges) and Web Application scans (authenticated user privileges). All vulnerabilities identified from the scans shall be resolved; tracked in the systems' Plan of Action and Milestones (POA&M); and submitted to the GSA OCISO.

i. Providing support to the Information System Security Manager (ISSM), of record appointed by the CISO.

j. Providing support to the Information Systems Security Officer (ISSO) of record, appointed by the CISO for each information system.

- k. Ensuring Information Assurance (IA) is included in management planning, programming budgets, and the IT Capital Planning process.
- l. Requiring written notification of point(s) of contacts within other Federal agencies or outside organizations that manage GSA systems.
- m. Ensuring that IT systems that handle privacy data meet the privacy and security requirements of the Privacy Act and IT information security laws and regulations. This includes [GSA Order CIO 1878.1](#), [GSA Order CIO 1878.2](#) and [NIST SP 800-53](#)
- n. Reviewing and approving Privacy Impact Assessments (PIAs) for their organizations.
- o. Supporting the security measures and goals described in Chapter 3(i) (Performance Measures) of this policy.
- p. Ensuring all incidents involving data breaches which could result in identity theft are coordinated through GSA IT's Office of the Chief Information Security Officer (OCISO) and the GSA Management Incident Response Team (MIRT) using the GSA breach notification plan per OMB Memorandum [M-07-16](#), Safeguarding Against and Responding to the Breach of Personally Identifiable Information, IT Security Procedural Guide: Incident Response (IR), [CIO-IT Security-01-02](#) and GSA Order, [CIO 9297.2B](#), [GSA Information Breach Notification Policy](#).
- q. Ensuring contingency and continuity of support plans are developed and tested annually in accordance with OMB Circular No. A-130, [NIST SP 800-34](#), Contingency Planning Guide for Information Technology Systems, and IT Security Procedural Guide: Contingency Planning, [OCIO-IT Security-06-29](#).
- r. Implementing detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in GSA business operations.
- s. Establishing physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.
- t. Ensuring access to systems by members of the GSA OIG as described in paragraph 16 of this chapter.
- u. Establishing appropriate system/organization unique rules of behavior for systems under their authority.
- v. Ensuring that IT systems that handle payment card data meet the security requirements of the in Payment Card Industry Data Security Standard.

8. Office of CISO Division Directors. OCISO Directors are the intermediary to the Authorizing Official for ensuring that security is implemented. The Director is the focal point for all IT system security matters for the IT resources under their responsibility. OCISO Directors report to the CISO. Responsibilities include:

a. Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO.

b. Reviewing and approving system assessments, prior to forwarding them to the Authorizing Official for approval and the CISO for concurrence.

c. Reviewing and approving assessment and authorization documents to be signed by the appropriate business line representatives and concurred by the appropriate OCISO personnel.

d. Ensuring the security measures and goals described in Chapter 3(i) Performance Measures of this policy are met by the organizations under their responsibility.

e. Ensuring GSA security and privacy awareness training requirements for individuals under their responsibility are complied with.

f. Creating security policies that achieve compliance to appropriately address new security requirements.

g. Advises individuals with IT Security responsibility on proper system security, security "Best Practices" and applicable laws and regulations.

9. Information Systems Security Manager (ISSM). The Information Systems Security Manager (ISSM) is the intermediary to the System Owner and the OCISO Director responsible for ISSO services. There is at least one ISSM per Authorizing Official. The ISSM reports to the OCISO Director for the systems under their authority. An individual appointed as ISSM for a system cannot also be assigned as the ISSO for the same system. Current listings of FISMA Contacts are located on InSite. Responsibilities include:

a. Ensuring adherence and proper implementation of GSA's IT Security Policy.

b. Providing guidance to the ISSOs.

c. Verifying annually the list of ISSOs and providing an updated designation letter to the Director for submission to the CISO when changes occur or designations expire.

d. Ensuring assessment and authorization support documentation is developed and maintained.

- e. Reviewing and coordinating reporting of Security Advisory Alerts (SAA), compliance reviews, security and privacy awareness training, incident reports, contingency plan testing, and other IT security program elements.
- f. Managing system assessments (including A&A package requirements **PCI DSS Report on Compliance (for IT systems that handle payment card data)**), and forwarding them to the Authorizing Official and OCISO Directors.
- g. Forwarding to the appropriate OCISO Director, copies of assessment and authorization documents to be signed by the appropriate individuals as required in A&A guidance.
- h. Supporting the security measures and goals described in Chapter 3(i) Performance Measures of this policy.
- i. Complying with GSA security and privacy awareness training requirements for individuals with significant security responsibilities.

10. Information Systems Security Officer (ISSO). The Information Systems Security Officer (ISSO) is the focal point for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches. An ISSO must be assigned for every information system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO cannot also be the ISSM for the same system. The ISSO must be knowledgeable of the information and processes supported by the system. The ISSO shall maintain accurate system inventories for information systems for which they have responsibility. A current list of ISSOs is located on InSite at: https://ea.gsa.gov/EAWEB/#!/FISMA_POC. Regional ISSOs (RISSOs) have the same responsibilities as designated ISSOs. Responsibilities include:

- a. Ensuring effective implementation of GSA's IT Security Policy.
- b. Ensuring the system is operated, used, maintained, and disposed of in accordance with documented security policies and procedures. Necessary security controls should be in place and operating as intended.
- c. Advising System Owners of risks to their systems and obtaining assistance from the ISSM, if necessary, in assessing risk.
- d. Assisting System Owners in completing and maintaining the appropriate security documentation including the system security plan.
- e. Assisting the Authorizing Official in the system assessment and authorization (processes) and creating and maintaining authorization documentation. The ISSO will assist the System Owner to develop and update the system security plan, manage and control changes to the system, and assess the security impact of those changes.

- f. Assisting the Authorizing Official, Data Owner and Contracting Officer / Contracting Officer Technical Representative in ensuring users have the required background investigations, the required authorization and need-to-know, and are familiar with internal security practices before access is granted to the system.
- g. Promoting information security awareness.
- h. Identifying, reporting and responding to security incidents.
- i. Reviewing and responding as appropriate to Security Advisory Alerts on vulnerabilities.
- j. Ensuring the user identification and authentication scheme used in the system is administered as intended.
- k. Ensuring media handling procedures are followed.
- l. Reviewing system security audit trails and system security documentation to ensure security measures are implemented effectively.
- m. Evaluating known vulnerabilities to ascertain if additional safeguards are needed; ensuring systems are patched, and security hardened.
- n. Beginning protective or corrective measures if a security breach occurs.
- o. Assisting in the development and maintenance of contingency plan and contingency plan test report documentation.
- p. Supporting the security measures and goals described in Chapter 3(i) Performance Measures of this policy.
- q. Complying with GSA security and privacy awareness training requirements for individuals with significant security responsibilities.
- r. Ensuring Privacy Impact Assessments (PIAs) are completed for IT systems that are new, under development, or undergoing major modifications which impact Privacy Act data.
- s. Working with the ISSM and System Owners to develop, implement, and manage POA&Ms for assigned systems IAW IT Security Procedural Guide: Plan of Action and Milestones (POA&M), OCIO-IT Security-09-44.
- t. Reviewing system role assignments to validate compliance with principles of least privilege.

u. Assisting the Authorizing Official in PCI DSS Implementation and certification for IT systems that handle payment card data, to include creating and maintaining PCI DSS documentation, and facilitating the self-assessment.

11. System Owners. System Owners (e.g. System Program Managers/Project Managers) are management officials within GSA who bear the responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk and privacy should rest with the System Owners. Responsibilities include:

- a. Ensuring effective implementation of GSA's IT Security Policy.
- b. Ensuring their systems and the data each system processes have necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM.
- c. Obtaining the security resources for their respective systems.
- d. Developing and implementing a configuration management plan for their respective systems.
- e. Using the advice of the ISSM and ISSO along with the approval of the Authorizing Official, selecting the mix of controls, technologies, and procedures that best fit the risk profile of the system.
- f. Participating in activities related to the assessment and authorization of the system to include security planning, risk assessments, security and incident response testing, and contingency planning and testing.
- g. Defining and scheduling software patches.
- h. Ensuring IT security and privacy requirements are included in IT contracts or contracts including IT.
- i. Ensuring implementation of privacy requirements for their system of record.
- j. Conducting PIAs on all systems to ascertain whether the system collects information on individuals or when new systems are developed, acquired, or purchased.
- k. Developing, implementing and maintaining an approved IT Contingency Plan which includes an acceptable Business Impact Analysis (BIA).
- l. Ensuring that information and system categorization has been established for their systems and data IAW FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

m. Conducting annual reviews and validations of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges).

n. Ensuring that for each information system, security is planned, documented, and integrated into the system development life cycle (SDLC) from the information system's initiation phase to the system's disposal phase.

o. Reviewing the security controls for their systems and networks annually as part of the FISMA review, when significant changes are made to the system and network and at least every three years or via continuous monitoring based on continuous monitoring plans reviewed and accepted by the GSA CISO.

p. Defining, implementing, and enforcing detailed separation of duties by ensuring that single individuals do not have control of the entirety of a critical process, roles, permissions, and/or responsibilities.

q. Ensuring that physical or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk.

r. Obtaining a written Authorization To Operate (ATO) following GSA Assessment and Authorization processes prior to making production systems operational and/or Internet accessible. Developing and maintaining the system security plan and ensuring that the system is deployed and operated according to the agreed-upon security requirements.

t. Ensuring that system users and support personnel receive the requisite security and privacy awareness training (e.g., instruction in rules of behavior) and assisting in the identification, implementation, and assessment of the common security controls.

u. Supporting the security measures and goals described in Chapter 3(i) Performance Measures of this policy.

v. Complying with GSA security and privacy awareness training requirements for individuals with significant security responsibilities.

w. Integrating and explicitly identifying security funding for information systems and programs into IT investment and budgeting plans.

x. Working with program officials and the system developer on the system's privacy issues, preparing a PIA report, obtaining the Program Manager's approval of the PIA report, and submitting the PIA report to the GSA Personnel Security Officer and GSA IT officials for review and approval.

- y. Coordinating with IT security personnel including the ISSM and ISSO and Data Owners to ensure implementation of system and data security requirements.
- z. Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems IAW IT Security Procedural Guide: Plan of Action and Milestones (POA&M), OCIO-IT Security-09-44.
 - aa. Ensuring proper separation of duties for GSA IT system maintenance, management, and development processes.
 - bb. Conducting annual assessments to review the effectiveness of control techniques, with an emphasis on activities that cannot be controlled through logical, physical, or compensating controls.
 - cc. Working with the Data Owner, granting access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.
 - dd. Working with Data Owners with assistance from the ISSO, will ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs, such as the annual IT Security & Privacy Act training curriculum.
 - ee. Working with Data Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities.
 - ff. Working with Data Owners to ensure that log data is archived for a period of not less than 180 days.
 - gg. Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities.
 - hh. Working with Data Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.
- ii. Working with the GSA Senior Agency Official for Privacy and Privacy Officer and legal counsel to determine the authority of any program or activity to collect PII.
- jj. Reviewing the security controls for its Payment Card systems and networks annually as part of the PCI DSS assessment, when significant changes are made to the system and network.
- kk. Working with the Office of the Chief Information Security Officer and Data Owners to respond to any information security incidents that impact the system or the data stored within the system.

II. Ensuring the GSA Records Management Program is adequately implemented.

12. Data Owners. The Data Owner/Functional Business Line Manager owns the information but not the system application or platform on which the information is processed. Responsibilities include:

- a. Determining the security categorization of systems based upon the FIPS Publication 199 levels and ensuring that System Owners are aware of the sensitivity of data to be handled.
- b. Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA.
- c. Working with the System Owner, with assistance from the ISSO, to ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs (such as the annual IT Security & Privacy Act and Sharing Information in a Collaborative Environment training curriculum).
- d. Reviewing access authorization listings and determining whether they remain appropriate at least annually.
- e. Ensuring protection of GSA's systems and data IAW GSA's IT Security Policy and the GSA Records Management Program.
- f. Ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data.
- g. Assisting in identifying and assessing the common security controls where the information resides.
- h. Ensuring information systems that allow authentication of users for the purpose of conducting Government business electronically (accessed via the Internet or via other external non-agency controlled networks, such as partner Virtual Private Networks (VPN)) complete an e-authentication risk assessment resulting in an authentication assurance level classification IAW [OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies](#).
- i. Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of system and data security requirements.
- j. Working with the System Owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities.

k. Working with the System Owner to ensure that log data is archived for a period of not less than 180 days.

l. Working with the System Owner to audit user activity for indications of fraud, misconduct, or other irregularities.

m. Working with the System Owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

o. Identifying the data assets to catalog in GSA's Enterprise Data Inventory (EDI) and for possible public release.

p. Working with the Office of the Chief Information Security Officer and System Owners to respond to any information security incidents that impact the system or the data stored within the system.

13. Contracting Officers (CO)/Contracting Officer's Representative (COR). The Acquisitions/Contracting Officer function is responsible for managing contracts and overseeing their implementation. For additional information refer to GSAM 539-7002 clauses 552.239 and 552.239-71. Personnel executing this function have the following responsibilities in regards to information security:

a. Collaborating with the CISO or other appropriate official to ensure that the agency's contracting policies adequately address the agency's information security requirements.

b. Coordinating with the CISO or other appropriate official as required ensuring that all agency contracts and procurements are compliant with the agency's information security policy.

c. Ensuring that all personnel with responsibilities in the agency's procurement process are properly trained in information security.

d. Working with the CISO to facilitate the monitoring of contract performance for compliance with the agency's information security policy.

e. Identifying and initiating contractor background investigations in collaboration with the GSA Personnel Security Officer.

f. Ensuring contracts and task orders for ISSM and ISSO services include performance requirements that can be measured.

g. Ensuring that all IT acquisitions include the appropriate security requirements in each contract and task order.

h. Ensuring that the appropriate security and privacy contracting language is incorporated in each contract and task order.

i. Maintaining the integrity and quality of the proposal evaluation, negotiation, and source selection processes while ensuring that all terms and conditions of the contract are met.

j. Ensuring new solicitations include the language of OMB Memorandum [M-07-18](#).

k. Ensuring all GSA contracts, Request for Proposals (RFP), and Request for Quotes (RFQ) involving Privacy Act information adhere to the Federal Acquisition Regulations ([FAR](#)) Privacy Act provisions (Subparts [24.1](#)) and include the specified contract clauses (Parts [52.224-1](#) and [52.224-2](#)), as appropriate.

l. Ensuring industry and Government information technology providers use Security Content Automation Protocol (SCAP) validated tools with the United States Government Configuration Baseline (USGCB) Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.

m. Ensuring new solicitations for all GSA IT systems includes the security contract language from [IT Security Procedural Guide: Security Language for IT Acquisition Efforts, OCIO-IT Security-09-48](#).

14. Custodians. Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. Responsibilities include:

a. Coordinating with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.

b. Providing and administering general controls such as back-up and recovery systems consistent with the policies and standards issued by the Data Owner.

c. Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the Authorizing Official.

d. Accessing data only on a need to know basis as determined by the Data Owner.

e. Providing the Office of the Chief Information Security Officer physical access to devices when needed as part of any incident response effort.

15. Authorized users of IT resources. Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA's IT Security Policy. Their responsibilities include:

- a. Complying with all GSA security policies and procedures.
- b. Complying with security and privacy awareness training, education, and awareness sessions commensurate with their duties.
- c. Reporting any observed or suspected security problems/incidents to their local IT Service Desk .
- d. Complying with background investigation policies.
- e. Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data.
- f. Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver, and removing PIV card before leaving their workstation.
- g. Ensuring Personally Identifiable Information (PII) and/or sensitive data stored on any workstations or mobile devices including, but not limited to, laptop computers, notebook computers, external hard drives, USB drives, CD-ROMs/DVDs, personal digital assistants is encrypted with GSA provided encryption. Employees and contractors may access PII remotely [i.e., remote access is when the individual is not physically located in a GSA facility (e.g., when the individual is teleworking)] unless explicitly prohibited by the GSA Senior Agency Official for Privacy (SAOP) and/or the Authorizing Official (AO) for the particular information system, in coordination with the Data Owner and/or the GSA Supervisor. All access shall only be from Government Furnished Equipment (GFE) or through an approved GSA virtual interface (i.e. Citrix and/or VDI). In addition, an individual shall not download or store PII on non-GFE. Approval to telework is at the discretion of the GSA Supervisor and/or Contracting Officer, as applicable, and in conformance with GSA Order [HCO 6040.1A, GSA Mobility and Telework Policy](#).
- h. Ensuring GSA managed computers that collect and store PII must adhere to all PII requirements.
- i. Utilizing assigned privileged access rights (power user, database administrator, web site administrator, etc.) to a computer based on need to know.

16. GSA Inspector General (IG). The GSA IG is the focal point for a statutory office within an organization that, in addition to other responsibilities, works to assess an organization's information security practices and identifies vulnerabilities and the possible need to modify security measures. The Office of Inspector General (OIG) completes this task by:

a. Detecting fraud or instances of waste, abuse, or misuse of an organization's funds.

b. Identifying operational deficiencies within the organization.

c. Performing annual independent FISMA evaluations.

d. Accessing GSA and contractor records. OIG auditors, investigators, inspectors, and attorneys must be provided access to all records, reports, reviews, documents, papers, and materials available to GSA and pertaining to agency programs and activities. When performing reviews of contractor records and proposals, access to information is provided by statute, contract terms, and agreements between the contractor and the Government. To facilitate the process of gaining access to information, auditors, investigators, inspectors, and attorneys carry credentials identifying them as OIG officials. In addition, the following procedures will be followed to allow OIG personnel access to GSA electronic systems:

(1) For the OIG, the point of contact will be the Assistant Inspector General for Auditing (AIGA) or his/her designees. For the Services and Staff Offices within GSA, the points of contact will be the Authorizing Official (AO) for each information system.

(2) The AIGA will notify the AO of the electronic system within his or her purview to which OIG personnel need access.

(3) The AO will inform the AIGA what the highest classification level is of information on the system and all security and privacy awareness training that is required of GSA and/or contractor personnel in order to access the system.

(4) The AIGA will designate the OIG personnel who are to be given access and ensure they have appropriate clearance levels.

(5) The AIGA will certify that each OIG person who may have access to the system has completed all security and privacy awareness training required of GSA personnel before access is granted.

(6) The AIGA will annually certify that each OIG person with access to a GSA system has a continuing need for access and has maintained up-to-date training requirements in connection with the System Owner's annual review and validation of systems users' accounts as described in paragraph 2.10 of this chapter.

(7) The AIGA will ensure and state that access is necessary for OIG personnel to accomplish assigned tasks IAW the OIG's organizational mission and functions. The following statement from the AIGA will suffice to establish that access is necessary for these purposes: "This access is requested to fulfill the OIG's statutory responsibility to conduct and supervise audits, inspections, and investigations relating to the programs and operations of GSA, and to promote economy, efficiency and effectiveness in the

administration of, and to prevent and detect fraud, waste, and abuse in GSA programs and operations.”

(8) With regard to requests for access to Privacy Act systems of records, the AIGA will ensure and certify that the OIG personnel who will be accessing the system have a need for the records in the performance of their duties. The statement shall suffice to establish that access to the system is consistent with the requirements of the Privacy Act.

(9) The AO will work with the System Owner to ensure access is granted promptly after the above steps have been completed. If access cannot be granted within fourteen (14) calendar days after completion of the above steps, the AO will inform his/her HSSO and the AIGA and will work with the AIGA to resolve any impediments to OIG access to the system. The Chief Information Officer, or designee, will assist as requested in resolving any issues.

(10) The System Owner will authorize OIG personnel to access GSA-owned information systems from the OIG’s accredited system. When possible under contractual terms, OIG personnel will be authorized access to contractor-owned information systems from the OIG’s accredited system.

(11) To the extent practicable, OIG personnel will not be granted access to other agencies’ owned or controlled records or information about other agencies and their employees that may be maintained in a GSA-controlled system, absent the other agency’s permission.

(12) The OIG will advise the AO immediately if circumstances change such that access is no longer needed; for example, if an individual with access leaves the OIG, or upon conclusion of the investigation/inspection/audit or other OIG purpose for which systems access was provided.

(13) OIG employees will have “read-only” access to all information in the system. OIG personnel will not be able to add to, delete, or modify the data in the system.

(14) Each OIG employee with access will use a unique identifier and password when accessing the system.

(15) Testing in support of an OIG review, whether manual or automated, shall not have an adverse effect on the operational production status of the IT system being reviewed other than the increase in usage/traffic due to additional users.

(16) OIG operational needs may preclude OIG staff from obtaining the required approvals prior to removal of personally identifiable information from GSA facilities. The following statement from the AIGA will suffice to establish that requirement is necessary for these purposes: “This access is requested to fulfill the OIG’s statutory responsibility

to conduct and supervise audits, inspections, and investigations relating to the programs and operations of GSA, and to promote economy, efficiency and effectiveness in the administration of, and to prevent and detect fraud, waste, and abuse in, GSA programs and operations.”

(17) Should the system be compromised by a reportable incident, and the access of OIG personnel be implicated in the incident, the System Owner will promptly notify the Inspector General in writing, and the Inspector General will take appropriate action with respect to the employee(s) responsible.

17. GSA Personnel Security Officer/Office of Human Resources Management. The GSA personnel security officer is responsible for the overall implementation and management of personnel security controls across GSA, to include integration with specific information security controls. As information security programs are developed, Chief officials should work to ensure this coordination of complementary controls. In consideration of information security, the personnel security officer has responsibility for:

- a. Developing, promulgating, implementing, and monitoring GSA personnel security programs.
- b. Developing and implementing position risk designation (including third-party controls), access agreements, and personnel screening, termination, and transfer procedures.
- c. Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.
- d. There shall be no waivers to background investigations for IT access for GSA employees or contractors. A favorable initial fitness/suitability determination shall be granted before access to the GSA network or any GSA IT system.

18. System/Network administrators. System/Network Administrators are responsible for:

- a. Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
- b. Implementing system backups and patching of security vulnerabilities.
- c. Utilizing privileged access rights (e.g., “administrator,” “root,” etc.) to a computer based on a need to know.
- d. Working with the Custodian/ISSO to ensure appropriate technical security requirements are implemented.

e. Ensuring System/Network administrators have separate Administrator and User accounts, if applicable (e.g., Microsoft Windows accounts). The Administrator privileged account must only be used when Administrator rights are required to perform a job function. A normal user account should be used at all other times.

f. Identifying and reporting security incidents and assisting the OCISO, in resolving the security incident.

g. Utilizing GSA provided Multifactor Authentication is being used to ensure strong authentication.

19. Supervisors. Supervisors are responsible for:

a. Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system.

b. Conducting annual reviews of staff training records to ensure annual IT Security Awareness, Privacy Act, Security Training, and application specific training was completed for all users. The records shall be forwarded to application ISSO/System Owners as part of the annual recertification efforts.

c. Coordinating and arranging system access requests for all new or transferring employees and for verifying an individual's need-to-know (authorization).

d. Coordinating and arranging system access termination for all departing or resigning personnel.

e. Coordinating and arranging system access modifications for personnel.

f. Documenting job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. Establishing formal procedures to guide personnel in performing their duties, with identification of prohibited actions.

CHAPTER 3: POLICY ON MANAGEMENT CONTROLS

This chapter provides the basic management control security policy statements for GSA systems. Management Controls deal with the overall control of the security program for GSA, including networks and systems. The policy statements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The manner in which these controls are implemented depends on the risks, sensitivity, and criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

1. According to NIST, the Management Controls are obtained from the following Control Families:

- Certification, Accreditation, and Security Assessments (CA)
- Planning (PL)
- Program Management (PM)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

2. The following paragraphs provide specific policy on controls for the security management of GSA systems.

a. Assign responsibility for security.

(1) A security management structure must be established and security responsibilities must be clearly assigned.

(2) Responsibility for the security of the IT system must be assigned to an Authorizing Official.

(3) Responsibility for ensuring security is implemented across the Services, Staff Offices, or Regions must be assigned, in writing, to an ISSM.

(4) Responsibility for each major application and general support system within the Services, Staff Offices or Regions must be assigned, in writing, to an ISSO.

b. Risk management.

(1) Authorizing Officials must implement a risk management process for all information systems using [NIST SP 800-30: Guide for Conducting Risk Assessments](#) and [GSA IT Security 06-30: Managing Enterprise Risk – Security Assessment and Authorization, Planning and Risk Assessment](#) and all identified A&A process procedural guides as required.

(2) Authorizing Officials must ensure risk assessments are performed and documented as part of assessment and authorization activities before a system is placed into production, when significant changes are made to the system and at least every three (3) years or via continuous monitoring based on [GSA CIO IT Security 12-66: Continuous Monitoring Program](#) that is reviewed and accepted by the GSA CISO.

(3) All information systems must use [NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories](#) and [FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems](#) to determine their security category (i.e. risk level) for confidentiality, availability and integrity.

(4) All information systems that allow authentication of users for the purpose of conducting government business electronically (accessed via the Internet or via other external non-agency controlled networks, such as partner VPN) complete an e-authentication risk assessment resulting in an authentication assurance level classification IAW OMB Memorandum [M-04-04](#), E-Authentication Guidance for Federal Agencies.

(5) Authorizing Officials must ensure that the risk management process includes contingency and continuity of support plans developed and tested annually IAW Office of Management and Budget (OMB) Circular No. A-130, NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, and [GSA CIO-IT-Security 06-29: IT Security Procedural Guide: Contingency Planning](#).

(6) All information systems must develop and maintain Plan of Action and Milestones (POA&M) in accordance with [IT Security Procedural Guide: Plan of Action and Milestones \(POA&M\)](#), [OCIO-IT Security-09-44](#). POA&Ms are the authoritative agency management tool for managing system risk and used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems. GSA must submit POA&Ms to OMB upon request.

(7) All FIPS 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test (or 'pentest') and provide an Independent Penetration Test Report documenting the results of the exercise as part of the Assessment and Authorization (A&A) package. NIST 800-53 R3 control CA-2(2) and NIST 800-53 R4 control CA-8 requires FIPS 199 High impact systems to complete penetration tests annually. The annual penetration tests can be completed internally and do not require an independent assessor. In addition, all Internet facing systems in the GSA CIO IT Security 12-66: Continuous Monitoring Program must conduct penetration testing annually. In addition, all systems undergoing the Lightweight ATO process must conduct penetration testing.

c. Review of security controls.

(1) Every IT system both government and contractor operated must undergo a security control assessment utilizing the current version of [NIST SP 800-53](#) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, and the annual requirements provided by the OCISO.

(2) The OCISO must submit, on behalf of the CIO, an agency-wide FISMA Report to OMB and specified congressional committees annually.

(3) An entity-wide IT security program must include compliance reviews to determine how well the over-all GSA security program meets the agency performance measures.

d. Lifecycle.

(1) GSA IT Security Policy must be incorporated into each phase of the lifecycle, (i.e., initiation, development/acquisition, implementation, operation and disposal) for all GSA information systems.

(2) System owners must use [NIST SP 800-64 Security Considerations in the Information System Development Life Cycle](#), [GSA Order CIO P 2140.3, Systems Development Life Cycle \(SDLC\) Policy](#), and the [GSA Solutions Life Cycle Handbook](#) as guides when managing security throughout the system's lifecycle.

(3) The Security Engineering Division (ISE) in the OCISO must participate in the Executive Business Case review process as a member of the Enterprise Architecture Review Board (EARB)

(4) The ISE must approve all contract documents, such as RFPs and SOWs prior to publication,

(5) The ISE must approve all Security Architecture designs prior to implementation.

e. Authorized processing.

(1) The AO must authorize, in writing, all information systems before they go into operation.

(2) All GSA information systems must be assessed and authorized at least every three (3) years or whenever there is a significant change to the system's security posture IAW [NIST SP 800-37](#), Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, and IT Security Procedural Guide: Managing Enterprise Risk, [OCIO-IT Security-06-30](#).

(3) As part of the assessment and authorization process, all systems must be categorized in accordance with FIPS PUB 199, and NIST SP 800-60. Risk Assessments must be performed IAW NIST SP 800-30. E-authentication risk assessments must be performed IAW OMB M-04-04. All controls must be implemented IAW FIPS PUB 200 and the current version of NIST SP 800-53. All controls must be documented in the system's security plan IAW NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems. All controls must be documented and tested IAW NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans and any other supplemental GSA guidance. In addition, contingency plans must be developed IAW NIST SP 800-34 and have been tested IAW GSA-CIO-IT Security 06-29 within the past year in order for the Authorizing Official to authorize the system to operate (i.e. accredit).

(4) A [Lightweight ATO](#) (aka Limited ATO) can be issued to a Low or Moderate impact system for an initial ninety (90) day period based on the results of a Pen Test. This can be extended up to a year for Moderate or a full three year ATO for low impact systems in the GSAIT organization, pursuing an agile development methodology AND residing on infrastructures that have a GSA ATO concurred by the GSA CISO or a FedRAMP ATO.

(5) Information systems with expiring Authorizations to Operate (ATO) may request a one-time extension of the current authorization for a period not to exceed one year from the date of ATO expiration if during this time the system will be decommissioned or to allow development of near real-time continuous monitoring capabilities to support ongoing authorization. ATO extensions must be supported by current vulnerability assessment results (operating system, database, and web (as applicable)) and POA&M identifying weaknesses from all sources. AOs must obtain approval from the CISO for the continuous monitoring plans of systems authorizations that have been extended. Plans must be approved within 6 months of the extension. New systems and systems that have undergone or are undergoing a significant change must adhere to the current GSA Risk Management Framework processes as documented in GSA CIO-IT Security-06-30.

(6) All GSA information systems must complete a Privacy Impact Assessment (PIA) as part of the assessment and authorization process. The PIA must be reviewed and updated annually or more frequently if there is a significant change to the system's privacy posture.

(7) Private sector cloud computing Software as a Service (SaaS) solutions that are implemented for limited duration and/or one time use; involve data already in the public domain or data that is non-sensitive and could be considered minimal impact; GSA would not be harmed regardless of the consequence of an attack or compromise, and the dollar cost for such a deployment does not exceed \$100,000 annually, may follow the streamlined assessment and authorization approach defined in IT Security Procedural Guide: Managing Enterprise Risk, OCIO-IT Security-06-30, for such

systems. AOs must consider Federal and agency information security requirements, and the S/SO security needs. An evaluation of the data and project scope must be performed to assure the conditions noted above are met. A review of the security controls and activities for such systems must be performed to assure the security controls and practices of the contractor are adequate before authorizing use and accepting residual risk.

f. System Security Plan (SSP).

(1) All information systems must be covered by a security plan IAW the current version of NIST SP 800-18.

(2) Update SSPs at least annually or when significant changes occur to the system.

g. Rules of the system.

(1) Authorized users must be provided written Rules of Behavior IAW GSA Order CIO 2104.1 before being allowed access into any GSA, non-public information system.

(2) The user must acknowledge receipt of these rules through a positive action.

h. System interconnections/information sharing.

(1) Written management authorization for system interconnection, based upon the acceptance of risk to the IT system, must be obtained from the AOs of both systems prior to connecting a system not under a single AO's control IAW NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc.

(2) If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system.

(3) All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be approved by the AO and concurred by the GSA CISO, and reviewed on an annual basis, at a minimum.

i. Performance measures. HSSOs, for their FISMA reportable systems, shall track the measures / goals presented by the CISO. AOs, System Owners, ISSMs, and ISSOs shall support these measures. The CISO shall periodically assess and report on the performance and goals.

j. Plan of Action and Milestones (POAMs). Capture all information security program and system weaknesses that require mitigation in the POA&M IAW GSA CIO-IT Security-09-44. POA&Ms shall be updated quarterly.

k. Contractors and outsourced operations. Implement appropriate safeguards to protect GSA information and information systems from un-authorized access throughout all phases of a contract. Review contracts to ensure that information security is appropriately addressed in the contracting language. GSA CIO-IT Security 09-48 establishes the security language for GSA IT acquisitions contracts involving contractors. All applicable NIST 800-53 controls should be put on contract (and a reasonable subset continuously monitored using guidance provided by the OCISO) for all contractor and outsourced operations. Given that the GSA IT security program is risk-based, it may not always make financial sense to mandate all NIST 800-53 IT security controls on an outsourced system. The System Program Manager and ISSO should make risk-based decisions on which controls could potentially be waived and then obtain concurrence from the Authorizing Official and the CISO.

l. Privacy Impact Assessments (PIAs). Conduct PIAs on all GSA information systems IAW OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 that includes, but is not limited to, the collection of new information in identifiable form (IIF). IIF is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, e-mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors, aka PII or when new information systems are developed, acquired, and/or purchased. The PIA must be reviewed and updated annually or more frequently if there is a significant change to the system's privacy posture IAW GSA Order CPO 1878.1 GSA Privacy Act Program.

m. Capital planning and investment. Integrate and explicitly identify funding for information systems and programs into IT investment and budgeting plans per NIST Special Publication 800-65: Integrating IT Security into the Capital Planning and Investment Control Process and GSA Order CIO 2135.2, GSA Information Technology (IT) Capital Planning and Investment Control. GSA's capital planning and investment control process must be used for the continuous selection, control, and evaluation of IT investments over their life cycles.

n. Enterprise Architecture (EA). Systems shall be implemented per the enterprise architecture principles in [CIO 2110.2 GSA Enterprise Architecture Policy](#). The principles contained in GSA Order CIO 2110.2 are consistent with OMB Circular A-130 which establishes the framework for architecture to address security controls for components, applications, and systems.

(1) In addition to the principles set forth in GSA Order CIO 2110.2, architecture practices cited in OMB's Federal Segment Architecture Methodology must be used during planning a new system or significant capability enhancement.

(2) GSA OCISO has determined that the implementation of enterprise architecture principles is provided as a common control by the Office of Enterprise Planning and Governance (IE). For additional details, please refer to the GSA Information Security Program Plan.

CHAPTER 4: POLICY ON OPERATIONAL CONTROLS

This chapter provides the basic operational control security policy statements for GSA systems. Operational Controls concern requirements to design, maintain, and use GSA systems in a secure environment. The policy statements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The manner in which these controls are implemented depends on the risks, sensitivity, and criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

1. According to NIST, the Operational Controls are obtained from the following Control Families:

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

2. The following paragraphs provide specific policy on controls for the operational security of the system.

a. Personnel security.

(1) Background investigation requirements for access to GSA information systems (including contractor operations containing GSA information) shall comply with GSA Order CIO P 2181.1 GSA HSPD-12. Contractors requiring non-routine access to IT systems (contractor summoned for an emergency service call) are not required to have a personnel investigation and are treated as visitors and must be escorted while in a GSA facility.

(2) Termination and Transfer Procedures must be incorporated into the authorization process for all information systems. Refer to the GSA-CIO-IT Security 03-23: Termination and Transfer Procedural Guide for additional details.

(3) Supervisors of GSA employees and CORs of GSA contractors must be responsible for coordinating and arranging system access requests for all new or transferring employees and for verifying an individual's need-to-know (authorization).

(4) Supervisors of GSA employees and CORs of GSA contractors must be responsible for coordinating and arranging system access termination for all departing or resigning personnel.

(5) User authorizations must be verified annually for all information systems.

(6) The Authorizing Official or their designee must grant remote access (i.e. external to GSA's network) privileges only to those GSA employees and contractors with a legitimate need for such access as approved.

(7) Employees and contractors shall have a favorable initial fitness/suitability determination and be in the process of receiving a Minimum Background Investigation (or comparable investigation) or higher to access PII. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or Contracting Officer (for contract personnel), Data Owner, and the System's Authorizing Official (AO). Each System's AO, with the request of the GSA Supervisor, Data Owner or Contracting Officer, shall evaluate the risks associated with each such request. To find Authorizing Officials go to <https://ea.gsa.gov/> and click on "Security" then "FISMA Systems – POC."

(8) There shall be no waivers to background investigations for IT access for GSA employees or contractors. A favorable initial fitness/suitability determination shall be granted before access to the GSA network or any GSA IT system.

b. Physical and environmental protections.

(1) Physical and environmental security controls must be commensurate with the level of risk and must be sufficient to safeguard IT resources against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

(2) GSA servers, routers, and other communication hardware essential for maintaining the operability of GSA systems and their connectivity to the GSA Network, must be placed in an isolated, controlled-access location (i.e., behind locked doors).

(3) Limit access to rooms, work areas/spaces, and facilities that contain agency systems, networks, and data to authorized personnel. A list of current personnel with authorized access shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

(4) Visitor access records shall be maintained for facilities containing information systems (except for those areas within the facility officially designated as publicly accessible). Visitor access records include: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; (vii) name and organization of person visited, and (viii) signature and name of individual verifying the visitor's credentials. Visitor access records shall be reviewed at least annually.

(5) Ensure that all agency systems and networks are located in areas not in danger of water damage due to leakage from building plumbing lines, shut-off valves, and other similar equipment to support meeting federal and local building codes.

(6) Install and ensure operability of fire suppression devices, such as fire extinguishers and sprinkler systems, and detection devices, such as smoke and water detectors, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

(7) Install and ensure operability of air control devices, such as air-conditioners and humidity controls, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

(8) Ensure that guidance provided in the GSA CIO-IT Security – 12-64: Physical and *Environmental Protection* for a secure environment for information systems, including physical access control, fire protection, emergency power, and alternate sites are implemented. Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

c. Production and input/output controls. Data (including relevant and pertinent documentation) must be protected against unauthorized access, tampering, alteration, loss, and destruction during production, input, output, handling, and storage. This protection must include clarification for labeling sensitive security documentation IAW GSA policies. Additional guidance may be found in GSA CIO-IT Security-12-63: System and Information Integrity.

d. IT contingency planning/continuity of support planning. Contingency planning focuses on the recovery and restoration of an IT system following a disruption. The contingency plan supports the agency Continuity of Operations Plan (COOP) required by HSPD-20, National Continuity Policy, ensuring that Primary Mission-Essential Functions continue to be performed during a wide range of emergencies. Contingency and continuity of support plans must be developed and tested annually for all IT systems in accordance with OMB Circular No. A-130, NIST SP 800-34, and GSA CIO-IT Security-06-29.

(1) A system specific IT contingency plan must be developed that identifies and addresses preventive controls, damage assessment procedures, plan testing and training procedures.

(a) The Security Engineering Division in the Office of the Chief Information Security Officer must participate in the Executive Business Case review process as a member of the Enterprise Architecture Review Board (EARB)

(b) The Security Engineering Division in the Office of the Chief Information Security Officer must approve of all contract documents, such as RFPs and SOWs prior to publication.

(c) The Security Engineering Division in the Office of the Chief Information Security Officer must approve of all Security Architecture Designs prior to implementation.

(2) Each contingency plan must include an approved BIA recovery strategy and documented procedures to maintain the plan.

(3) Personnel supporting FIPS 199 Low, Moderate and High impact systems with contingency planning responsibilities shall be trained in their contingency roles and responsibilities with respect to the information system annually with refresher training every three years.

(4) The contingency plan must be annually tested IAW GSA CIO-IT Security-06-29.

(5) Continuity of operations plan (COOP) contact lists which only contain a person's name and home phone number are exempt from GSA IT security policy requirements in this policy. COOP contact lists kept on an electronic device that is password protected (other Government approved Smart Phone devices, laptop, USB drive) do not require written permission or encryption. Paper "cascade lists" limited to name and home phone number that are maintained for the purpose of emergency employee accountability are permissible with the approval of those individuals listed. All paper and other media should be kept in a locked facility or an otherwise secure location when not in use.

(6) The contingency plan must be updated annually to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

e. Hardware and software maintenance.

(1) The availability and usability of GSA equipment and software must be maintained and safeguarded to enable agency objectives to be accomplished.

(2) Lost or stolen GSA IT assets must be immediately reported to the IT Service Desk.

(3) All information systems must be securely hardened and patched before being put into operation and while in operation.

(4) Maintenance of agency hardware and software must be restricted to authorized personnel.

(5) Hardware and software must be tested in a non-production environment to identify adverse effects on system functionality, be documented, and approved prior to promotion to production.

(6) In GSA facilities, only approved Government Furnished Equipment (GFE) is allowed connection (e.g., Ethernet) to the network unless specifically approved by the General Support System Authorizing Official. All non-GFE will be given Internet only access, if possible.

(7) All GFE, to include hardware, software and COT applications, must be approved through the GSA Helpdesk approval process prior to procurement.

(8) Ensure that maintenance activities of hardware and software are IAW with GSA-IT-Security 10-50: Maintenance.

f. Data integrity.

(1) Data integrity and validation controls must be used on all information systems that require a high degree of integrity.

(2) All information systems must have up-to-date virus protection software.

(3) Ensure that data integrity is protected IAW GSA CIO-IT Security-12-63: System and Information Integrity.

g. Documentation. Security related documentation must be obtained or created to describe how security mechanisms are implemented and configured within the IT system. This includes but is not limited to:

- System Security Plan
- Configuration Management Plan
- Contingency Plan
- Privacy Impact Assessments

h. Security and privacy awareness, training, and education.

(1) A security and privacy awareness, training and education program must be established by the OCISO to ensure all GSA, other agency, and contractor support staff involved in the management, design, development, operation, and use of IT systems are aware of their responsibilities for safeguarding GSA systems and information.

(2) All GSA employees and contractors (internal and external*) must provide verification that Security Awareness Training and Privacy Training approved by GSA has been completed within 30 days of notification to complete the training and annually thereafter.

(3) All GSA employees and contractors (internal and external*), who have significant information security responsibilities as defined by OPM 5 CFR Part 930 and GSA IT security training policy, must complete specialized IT security training as defined in the policy.

(4) Failure to comply with annual awareness and specialized IT security training requirements will result in termination of access to GSA information systems. Authorizing Officials can terminate system accounts.

(5) Privacy 201 training is for managers, supervisors and employees that receive privacy data in the course of conducting GSA business. All employees and contractors shall complete "IT Security Awareness and Privacy 101 Training," "Privacy Training 201," and the "Sharing in a Collaborative Environment" training before being provided access to any PII, as defined in OMB Memorandum M-07-16 and M-10-23.

* An external contractor is defined as someone who has access to GSA information but doesn't have a GSA e-mail account.

i. Incident response capability.

(1) Every S/SO/R must establish a security incident response capability for detecting, reporting, and responding to security incidents.

(2) All authorized IT users must be trained annually to promptly report suspected vulnerabilities, security violations, and security incidents to their IT Service Desk. Refer to GSA-CIO-IT Security 01-02 for additional details.

(3) ISSOs must report security incidents through the IT Service Desk to the CISO IAW GSA CIO-IT Security-01-02. The OCISO shall then report incidents to the GSA Office of Inspector General IAW that Procedural Guide.

(4) All incidents involving the loss or theft of GSA hardware, software, and/or information in physical form, occurring in GSA Federal facilities, must be reported to the GSA OIG. The GSA OIG as appropriate will coordinate reporting to the Federal Protective Service, the local police, or other law enforcement authority with jurisdiction. Similar incidents occurring outside of Federal facilities must first be reported to the local police that has jurisdiction and to the OIG upon returning to the office. Government approved Smart Phone devices lost or stolen outside of GSA Federal facilities are not required to be reported to local police but must be reported to the OIG upon returning to the office. To report an incident, call the national hotline at 1(800) 424-5210 (Toll free). In addition, the incident should always be reported to the IT Service Desk. All incidents involving personally identifiable information in electronic or physical form must be reported to the GSA OCISO via the IT Service Desk within one hour of discovering the incident. GSA employees, contractors, and authorized users shall report all incidents to the IT Service Desk. There should be no distinction between suspected and confirmed

breaches. The OCISO shall promptly notify the GSA OIG of any incidents involving personally identifiable information.

(5) Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic) shall follow reporting and response procedures as defined in GSA Order CIO 9297.2B, GSA Information Breach Notification Policy. Refer to GSA Order CIO 9297.1 GSA Data Release Policy, for non-releasable information to the public or persons other than the employee, except when required by law (e.g., court order). See also Chapters 7 and 8 of GSA Order CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

(6) FIPS 199 Moderate and High impact systems must annually test the security incident response capability to determine the incident response effectiveness.

j. Security advisory alert handling.

(1) Office of the CISO must create procedures to share common threats, vulnerabilities, and incident related information with the appropriate organizations.

(2) ISSMs and ISSOs must report on the status of security advisory alerts to the Office of the CISO upon request.

k. Media protection.

(1) All GSA data from information system media, both digital and non-digital must be sanitized in accordance with methods described in IT Security Procedural Guide: Media Protection Guide, OCIO-IT Security-06-32, before disposal or transfer outside of GSA.

(2) Restrict access to information system media (e.g., disk drives, diskettes, internal and external hard drives, and portable devices), including backup media, removable media, and media containing sensitive information to authorized individuals.

(3) Physically control and securely store information system media within controlled areas.

(4) Protect digital media during transport outside of controlled areas using a certified FIPS 140-2 encryption module; non-digital media shall follow GSA personnel security procedures.

I. Configuration management.

(1) A system configuration management plan must be developed, implemented, and maintained for every IT system managed by GSA.

(2) All information systems must be securely hardened and patched before being put into operation and while in operation.

(3) GSA information systems, including vendor owned / operated systems on behalf of GSA, must configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Where a GSA benchmark exists, it must be used. GSA benchmarks may be exceeded but not lowered.

(4) Develop the configuration management plan IAW GSA-CIO-IT-Security-01-05.

m. Firewall access.

(1) The Office of the Chief Information Security Officer must approve all requests for access through the GSA Firewall. Firewall change requests must follow the process outlined in IT Security Procedural Guide: Firewall Change Request, OCIO-IT Security-06-31. This includes changes to desktop firewall and intrusion prevention systems.

(2) The Office of the Chief Information Security Officer will block access to all external sites deemed to be a security risk to GSA. Exceptions to this policy must be approved by the CISO.

Note: Detailed guidance regarding firewall access is available in GSA-CIO-IT-Security-06-31: Firewall Change Request.

n. Monitoring.

(1) Obtaining access to GSA resources must constitute acknowledgment that monitoring activities may be conducted.

(2) Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring.

(3) All GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems indicating the system is subject to monitoring.

(4) Controls shall be put in place to monitor or detect changes or updates to systems that are outside the parameters of a system's baseline operating characteristics. This includes the ability to monitor resource usage and allocation.

(5) Audit user activity for indications of fraud, misconduct, or other irregularities.

(6) Document all phases of monitoring activity including:

(a) Monitoring procedures. The procedures must include specific steps to be taken and protocol to be applied when reviewing audit data.

(b) Response procedures. Procedures must be documented for responses to detected irregularities.

(c) Review of user activity. Thorough documentation on reviews conducted on audit data must be generated and stored IAW the GSA Record Management Program or for not less than 3 years.

Note: Detailed guidance regarding monitoring is available in GSA-CIO-IT-Security-12-63: System and Information Integrity, GSA-CIO-IT-Security-01-02: Incident Response, GSA-CIO-IT-Security-01-05: Configuration Management, GSA-CIO-IT-Security-01-08: Audit and Accountability, GSA-CIO-IT-Security-01-07: Access Control.

o. Software and digital media acceptable use.

(1) Users of GSA IT resources must use only software that is properly licensed and registered for GSA use.

(2) All GSA users must abide by software and digital media copyright laws and must not obtain, install, replicate, or use unlicensed software and digital media.

(3) Users of GSA IT resources must obtain all software from GSA sources and must not download software from the Internet without prior permission from the appropriate ISSO, as downloading software from the Internet may introduce viruses/worms to the GSA network.

(4) Users must not install any software or hardware without approval through the EARC process.

(5) Users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise GSA resources unless authorized by the appropriate ISSO. Examples of such tools include those that defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.

(6) Users must not install, download, or run peer-to-peer software. Software that has peer-to-peer file sharing technology built in may be approved by OCISO if the file sharing functionality has been limited or disabled.

p. E-mail, social media and internet acceptable use.

(1) GSA provides access to e-mail and Social Media for Government business. However, users may occasionally make personal use of e-mail and Social Media that involves minimal expense to the Government and does not interfere with government business. Prior to establishing an official GSA Social Media presence, users must inform the Office of Communications and Marketing's (OCM) Enterprise Web Management (EWM) group which can monitor and assist with GSA branding and other aspects related to dealing with the public.

(2) Users must not use e-mail or Social Media for any activity or purpose involving classified data.

(3) Users must avoid the following prohibited e-mail and Social Media usages:

(a) Transmitting unsolicited commercial announcements or advertising material, unless approved by management in advance.

(b) Transmitting any material pertaining to GSA, the Federal Government, or any agency employee or official that is libelous or defamatory.

(c) Transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, un-authorized mass mailings, or intentionally sending a virus/worm.

(4) Personal use of Government IT systems for Internet access must be kept to a minimum and must not interfere with official system use or access.

(5) Users must avoid prohibited Internet usages including:

(a) Unauthorized attempts to break into any computer, whether belonging to GSA or another organization.

(b) Browsing sexually explicit, gambling sites or hate-based web sites.

(c) Using Internet access for personal gain (i.e., making use of GSA resources for commercial purposes or in support of for profit activities such as running a private business).

(d) Theft of copyrighted or otherwise legally protected material, including copying without permission.

(e) Sending or posting sensitive material such as GSA building plans or financial information outside of the GSA network.

(f) Automatically forwarding e-mail messages from GSA e-mail addresses to any non-Federal e-mail account(s) or address(es).

(g) Sending e-mail messages including sensitive information, such as PII, as deemed by the Data Owner, without GSA provided encryption. Certified encryption modules must be used IAW FIPS PUB 140-2, Security requirements for Cryptographic Modules.

(6) If PII needs to be e-mailed outside the GSA network encryption is required. Instructions can be found on the privacy web page in the section "Documents for Download." Your e-mail will be blocked if Social Security Numbers are sent unencrypted.

(7) GSA prohibits an employee or contractor supporting GSA from creating or sending information using a non-official GSA electronic messaging account unless: (1) copies of the message is sent to an official GSA electronic messaging account of the employee or contractor in the original creation or transmission of the record, or (2) a complete copy of the message or record is forwarded to an official GSA electronic messaging account of the employee or contractor not later than 20 days after the original creation or transmission of the record. Additional guidance regarding GSA E-Mail Policy is available in GSA Order CIO 2160.2 GSA Electronic Messaging and Related Services. GSA Order ADM 7800.11, Personal Use of Agency Office Equipment. GSA Order CIO 2104.1, GSA Information Technology (IT) General Rules of Behavior and GSA Order CIO P 2165.1, GSA Internal Telecommunications Management. Detailed guidance on Social Media is available in The Social Media Navigator, GSA's Guide to the Use of Social Media, April 2011 or current.

q. Portable storage devices.

(1) All agency data on portable storage devices (e.g., USB flash drives, SD cards, external hard drives) must be encrypted with a FIPS 140-2 certified encryption module.

(2) Users shall follow the requirements of Chapter 4, Paragraph i, Subparagraph 4 of this chapter with regard to PII or other data deemed sensitive by the Data Owner.

(3) Users must secure portable storage devices using the same policies and procedures as paper documents as proscribed by the Office of Human Resources Management (OHRM) policies.

(4) Users must protect portable storage devices in the same manner as a valuable personal item and should not leave unattended in public places, automobiles, etc.

(5) Users must immediately report lost or stolen portable storage devices to the appropriate ISSO or IT Service Desk. Reference Chapter 4, Paragraph i, Subparagraph 5 for reporting requirements to the OIG.

r. Mobile devices (smartphones/tablets). GSA users must secure mobile devices, like all enterprise devices, against a variety of threats. This includes handling PII as described in Chapter 4, Paragraph 4, subparagraph w of this chapter, securing the devices, and reporting lost or stolen devices. Included in the definition of 'Mobile devices' are smartphones and tablets. Excluded in the definition of mobile devices are laptops since the security controls for laptops are quite different from smartphones. Also excluded in the definition are basic cell phones due to the limited security options available and their limited threat. GSA has outlined information on mobile devices at: <https://sites.google.com/a/gsa.gov/mobileinfo/>. The [IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67](#) is designated as the GSA Policy on mobile devices and applications and provides specific information, including:

(1) Government issued devices.

(a) GSA uses centralized mobile device management (MDM) to manage the configuration and security of mobile devices. GSA provisions and activates MDM on each mobile device before issuing to users.

(b) GSA organizations must define procedures to periodically monitor mobile device security to verify compliance with GSA requirements.

(c) GSA's MDM ensures appropriate security including: encryption, application controls, passwords usage, remote locking, remote wiping, operating system protection.

(d) Users must not connect to GSA resources without complying with the requirements which the Guide describes.

(2) Personally owned mobile devices.

(a) GSA has implemented a Bring Your Own Device (BYOD) policy that allows users to connect non-GSA procured devices to GSA resources.

(b) [IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67](#) is designated as the GSA policy on mobile devices and applications, and details the steps necessary to use a personally owned mobile device, which include:

1. GSA will install MDM on the device and enforce control security settings, including password usage, encryption, and inactivity timeout.

2. GSA will ensure that GSA can wipe the device clean if it is lost or stolen or after repeated unsuccessful attempts at logon.

3. GSA will not support personally owned mobile devices.

4. Users must agree to and sign a GSA Personal Device Usage Agreement and the [GSA Rules of Behavior for Personally Owned Mobile Devices](#).

s. Peer-to-peer networking and instant messaging.

(1) The installation or use of peer-to-peer networking software is prohibited on GSA computers and the GSA network. Software that has peer-to-peer file sharing technology built in may be approved by OCISO if the file sharing functionality has been limited or disabled.

(2) The installation or use of unauthorized instant messaging (IM) software is prohibited. (i.e., must use an approved GSA standard).

t. Separation of duties (FIPS 199 Moderate and High Impact Systems Only).

(1) Responsibilities with a security impact must be shared among multiple staff by enforcing the concept of separation of duties, which requires that individuals do not have control of the entirety of a critical process.

(2) Define and implement detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in departmental business operations.

(3) Every S/SO/R must consider how a separation of duties conflict can arise from shared access to applications and systems. Specifically, application programmers and configuration management personnel should not generally have concurrent access to the development and production environment. Failure to segregate access to source code and production code increase the risk that unauthorized modifications to programs may be implemented into production systems, which could introduce vulnerabilities and negatively impact the integrity and availability of data generated and stored in the system.

(4) Document job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. By clearly documenting position responsibilities and functions, employees are positioned to better execute their duties IAW policy.

(5) Establish formal procedures to guide personnel in performing their duties, with identification of prohibited actions.

(6) Duties shall be segregated among users so that the following functions shall not generally be performed by a single individual:

(a) Data entry and verification of data. Any data entry or input process that requires a staff member to inspect, review, audit, or test the input to determine that the input meets certain requirements should not permit the same individual to both enter and verify the data. The objective is to eliminate self-certification or verification of data input or entry procedures. Note that this could be an automated or manual process and is not limited to financial transactions.

(b) Data entry and its reconciliation to output. Any data entry or input process that requires reconciliation or matching of transactions to identify discrepancies should not permit the same individual to both enter and reconcile data.

(c) Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information).

(d) Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).

(7) Ensure proper separation of duties for GSA IT system maintenance, management, and development processes.

(8) Information systems must enforce separation of duties through assigned access authorizations.

(9) Since critical processes can span separate and distinct applications and systems, each Service, Staff Office, and Region (S/SO/R) will take a macro view of existing roles to define and establish incompatibilities and separation of duties conflicts across an entire business process. This means examining roles that may span multiple IT systems or applications to uncover conflicts that may not be immediately apparent (e.g., an individual has permissions to create and/or modify vendor data in a General Ledger system and the ability to create invoices and purchase orders in an Accounts Payable system).

(10) Every S/SO/R must establish physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.

(11) Conduct annual assessments to review the effectiveness of control techniques, with an emphasis on activities that cannot be controlled through logical, physical, or compensating controls. The reviews determine whether in-place control techniques are maintaining risks within acceptable levels (e.g., periodic risk assessments).

(12) Review access authorization listings to determine whether they remain appropriate at least annually.

(13) Conduct annual reviews of staff training records to ensure annual Privacy Act, Security Training, and application specific training was completed for all users. The records shall be forwarded to application ISSO/System Owners as part of the annual recertification efforts.

u. Least privilege.

(1) Information systems must operate in such a way that they run with the least amount of system privilege needed to perform a specific function and that system access is granted on a need to know basis.

(2) Privileged rights including but not limited to “administrator,” “root,” and “power user” shall be restricted to authorized employees and contractors as approved by the AO.

(3) Information systems must be configured to the most restrictive mode consistent with operational requirements and IAW appropriate procedural guides from NIST and/or GSA to the greatest extent possible. Implemented configuration settings should be documented and enforced in all subsystems of the information system.

v. Remote access/end point security.

(1) All desktop or laptop computers, including personal devices, connecting remotely to GSA must have anti-virus software running with the latest signature files, a firewall installed and running, and all security patches installed. Failure to have current security signatures or patches may result in loss of access to the GSA network or data.

(2) All computers accessing GSA through a GSA Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec) Virtual Private Network (VPN) must allow an endpoint device that checks for the presence of a client firewall, up to date virus protection software and up to date patches. The endpoint device must also verify the absence of malicious software (e.g., Trojans, worms, malware, spyware, etc.) on the client machine. Machines that fail this scan will not be allowed access to the GSA network or any GSA IT resources.

(3) Only GSA GFE that is determined to be properly secured (based on the scans noted above) will be allowed unrestricted remote access to the GSA network.

(4) Personal computers and/or contractor computers will only be allowed access to the Citrix Netscaler and will not have the ability to map local drives (contingent on passing the security scans noted in paragraph b). No PII or other data deemed sensitive by the Data Owner shall be stored on non-GFE.

(5) In special cases for remote administration and maintenance tasks, contractors will be allowed restricted IPSEC access to specific GSA IP addresses (contingent on passing the security scans noted in paragraph b).

w. Personally Identifiable Information (PII). The following security requirements apply to the protection of PII.

(1) If it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants, PII must be encrypted using a FIPS 140-2 certified encryption module. An employee or contractor shall not physically take PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or access remotely (i.e., from locations other than GSA facilities), without written permission from the employee's supervisor, the Data Owner, and the IT system Authorizing Official. Approvals shall be filed with the employee's supervisor. This applies to electronic media (e.g., laptops, USB drives), paper, and any other media (e.g., CDs/DVDs) that may contain PII.

(2) PII shall be stored on network drives and/or in application databases with proper access controls (i.e., User ID/password) and shall be made available only to those individuals with a valid need to know.

(3) Log all computer-readable data extracts from databases holding PII and verify each extract including PII that has been erased within 90 days or if its use is still required.

(4) Creation of computer-readable data extracts that include PII shall be maintained in an official log including creator, date, type of information, and user.

(5) If PII needs to be transmitted over the Internet, it must be sent using encryption methods defined in Chapter 5, Paragraph 2, Subparagraph g of this IT security policy.

(6) Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic) shall follow reporting and response procedures as defined in GSA Order CIO 9297.2B, GSA Information Breach Notification Policy. Refer to GSA Order CIO 9297.1 GSA Data Release Policy, for non-releasable information to the public or persons other than the employee, except when required by law (e.g., court order). See also Chapters 7 and 8 of GSA Order CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

(7) GSA managed computers that collect and store PII must adhere to all PII requirements.

(8) If PII needs to be e-mailed outside the GSA network encryption is required. Instructions can be found on the privacy web page in the section "Documents for Download." Your e-mail will be blocked if Social Security Numbers are sent unencrypted.

(9) If PII needs to be sent by courier, printed, or faxed several steps should be taken. When sending PII by courier mark "signature required" when sending documents. This creates a paper trail in the event items are misplaced or lost. Don't let PII documents sit on a printer where unauthorized employees or contractors can have access to the information. When faxing information, use a secure fax line. If one is not available, contact the office prior to faxing, so they know information is coming, and contact them after transmission to ensure they received it. For each event the best course of action is limit access of PII only to those individuals authorized to handle it, create a paper trail, and verify information reached its destination.

(10) Comply with security and privacy awareness training requirements for employees and contractors (internal and external). All employees and contractors shall complete "IT Security Awareness and Privacy 101 Training," "Privacy Training 201," and the "Sharing in a Collaborative Environment" training before being provided access to any PII, as defined in OMB Memorandum M-07-16 and M-10-23.

(11) Ensure employees and contractors have the proper background investigation before accessing PII.

(12) Employees and contractors may access PII remotely [i.e., remote access is when the individual is not physically located in a GSA facility (e.g., when the individual is teleworking)] unless explicitly prohibited by the GSA Senior Agency Official for Privacy (SAOP) and/or the Authorizing Official (AO) for the particular information system, in coordination with the Data Owner and/or the GSA Supervisor. All access shall only be from Government Furnished Equipment (GFE) or through an approved GSA virtual interface (i.e. Citrix and/or VDI). In addition, an individual shall not download or store PII on non-GFE. Approval to telework is at the discretion of the GSA -Supervisor and/or Contracting Officer, as applicable, and in conformance with GSA Order HCO 6040.1A.

(13) Employees and contractors shall have a favorable initial fitness/suitability determination and be in the process of receiving a Minimum Background Investigation (or comparable investigation) or higher to access PII. The authority and access shall be determined by the appropriate GSA Supervisor (for GSA employees) or Contracting Officer (for contract personnel), Data Owner, and the System's Authorizing Official (AO). Each System's AO, with the request of the GSA Supervisor, Data Owner or Contracting Officer, shall evaluate the risks associated with each such request. To find Authorizing Officials go to <https://ea.gsa.gov/> and click on "Security" then "FISMA Systems – POC."

(14) There shall be no waivers to background investigations for IT access for GSA employees or contractors. A favorable initial fitness/suitability determination shall be granted before access to the GSA network or any GSA IT system.

(15) Employees and contractors working with PII shall verify callers' identity before discussing or providing any PII to individuals on the telephone. The verification technique shall be documented and approved by the GSA SAOP in advance of the discussion or provision of any PII.

(16) Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic), shall follow reporting and response procedures as defined in GSA Order CIO 9297.2B. GSA Information Breach Notification Policy. Refer to GSA Order CIO 9297.1 GSA Data Release Policy for non-releasable information to the public or persons other than the employee, except when required by law (e.g., court order). See also Chapters 7 and 8 of GSA Order CIO P 2180.1. GSA Rules of Behavior for Handling Personally Identifiable Information (PII).

x. Guest wireless access.

(1) A GSA Guest Wireless Network has been established in the Regional and Central Office Buildings to allow non-Government Furnished Equipment (GFE) access only to the Internet and GSA resources that are available to the general public (www.gsa.gov). It is intended to be a service for customers of the agency, as well as vendors performing official business on site.

(a) Guest wireless accounts are not ENT accounts.

(b) The User ID will change weekly

(c) The Password is posted on InSite.

(d) The password will be changed monthly.

(e) Guest wireless traffic will be subject to the same content filtering as traffic on the production network.

(2) All non-GFE/workstations connected to the GSA Network shall only be allowed access to the Internet (example: .guest network only, no access allowed to the GSA resources).

y. International travel policy for Portable Electronic Devices (PED). The widespread use of PEDs as stand-alone, networks and remote access devices, present special security concerns not limited to laptops, cell phones, thumb drives, Personal Data Assistants (PDA), tablets, and pagers. Vulnerabilities of these devices while on international travel warrant specific controls to protect the GSA network. GFE must not be taken on international travel without prior approval from the individual's supervisor and OMA.

(1) Individuals with a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance must contact OMA prior to any international travel.

(2) OMA will provide direction on foreign contact, security precautions, mobile devices, etc.

(3) GSA employees (with the exception of the OIG employees) that hold a National Security clearance, and at the discretion of OMA, shall be issued loaner devices by GSA IT when traveling outside the United States or European Union, or any area deemed to have an elevated risk during the period of travel. The loaner devices must be returned to GSA IT immediately upon the employee's return. These loaner devices shall be wiped immediately by GSA IT to ensure no data remains resident on the system(s) issued. Due to technical security controls in place for all mobile devices (encryption and, mobile device management), personnel in Public Trust positions are not required to follow this provision unless deemed to be required by OMA to provide additional safeguards to data these personnel may access.

CHAPTER 5: POLICY ON TECHNICAL CONTROLS

This chapter provides the basic technical control security policy statements for GSA systems. Technical Controls provide specific guidance on security controls and technical procedures used to protect GSA IT resources. The policy statements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The manner in which these controls are implemented depends on the risks, sensitivity, and are criticality associated with the specific systems and data involved. In some cases, basic security policy controls may need to be modified or supplemented in order to address application-specific or system-specific requirements.

1. According to NIST, the Technical Controls are obtained from the following Control Families:

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)

2. The following paragraphs provide specific policy on controls for identification and authentication, access control, auditing, and others.

a. Identification and authentication. All GSA systems must incorporate proper user identification and authentication methodology. Refer to the GSA-CIO-IT-Security-01-01: Identification and Authentication Procedural Guide for additional details. For mobile devices, refer to Chapter 4.

(1) Authentication schemes for Moderate and High Impact systems must utilize multifactor authentication using two or more types of identity credentials (e.g. passwords, SAML 2.0 biometrics, tokens, smart cards, one time passwords) as approved by the Authorizing Official and in accordance with the security requirements in the subparagraphs of this paragraph.

(2) An authentication scheme using passwords as a credential must implement the following security requirements:

(a) Passwords must contain a minimum of eight (8) characters which include a combination of letters, numbers, and special characters. Accounts used to access USGCB compliant workstations must contain a minimum of sixteen (16) characters but do not have to contain a combination of letters, numbers, and special characters.

(b) Information systems must be designed to require passwords to be changed every 90 days.

(c) Information systems must automatically lockout users after not more than ten (10) failed access attempts during a 30 minute time period. Accounts must remain locked for a minimum of 30 minutes for the next login prompt.

(d) Passwords for all mobile devices such as GSA approved smart phones, iPads, and tablets must be a minimum of 6 characters. The six character password requirement also applies to personal mobile devices accessing GSA data or systems.

(e) Passwords must not be stored in forms (i.e. Windows dialog boxes, web forms, etc.).

(f) All default passwords on network devices, databases, operating systems, etc. must be changed.

(g) Other than default or one time use passwords, passwords must never be sent via e-mail, regular mail, or interoffice mail.

(h) User IDs and passwords must never be distributed together (i.e. same e-mail, regular mail, interoffice mail, etc.).

(i) Users must be authenticated before resetting or distributing a password.

(4) Systems with an authentication assurance level of 2 or above, used by federal employees or contractors must accept federal Personal Identity Verification (PIV) cards and verify them in accordance with guidance in OMB M-11-33.

(5) All users issued Government Furnished Equipment are required to log into the workstation using a GSA issued PIV credential. The following groups of users are exempt from this requirement:

(a) A Federal employee on detail to GSA, issued a PIV from the employees assigned Agency

(b) Any employee or contractor expected to be employed for less than 180 days and not issued a PIV

(c) Any person with a disability that does not allow the individual to utilize a PIV card and laptop.

(d) Any user with a PIV that is lost, forgotten at home, or damaged in any way, may contact the IT Service Desk (ITSD) to request a temporary exception to the above requirement, not to exceed forty-five (45) days.

(6) Systems with users who are agency business partners or the general public, and who register or log into the system, must accept credentials issued by identity providers who have been certified by federally approved Trust Framework Providers.

(7) Authentication methods for applications and systems may use the authentication mechanisms provided by the general support system if deemed appropriate by the Authorizing Official.

(8) E-commerce and publicly accessible systems must incorporate identification and authentication mechanisms commensurate with their security risks and business needs and may differ from the security requirements set forth by this policy. In such cases the identification and authentication mechanisms must be approved by the AO in writing and concurred by the OCISO.

(9) One time use passwords must expire in twenty-four (24) hours.

(10) User IDs and passwords must never be distributed together, whether in the same e-mail, via interoffice mail, or postal mail.

(11) Users must be authenticated before resetting or distributing a password.

(12) User IDs shall be unique to each authorized user.

(13) All GSA workstation and mobile devices shall initiate a session lock after 15 minutes of inactivity. The session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication.

(14) FIPS 199 Moderate and High impact systems shall automatically terminate temporary and emergency accounts after no more than ninety (90) days.

(15) FIPS 199 Moderate and High impact systems shall automatically disable inactive accounts after ninety (90) days.

(16) FIPS 199 Moderate and High impact systems shall automatically terminate a remote access connection and Internet accessible application session after thirty (30) minutes of inactivity. The time will be thirty (30) – sixty (60) minutes for non-interactive users. Static web sites, long running batch jobs and other operations are not subject to this time limit.

(17) Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module. SSL/TLS implementation must be IAW [SSL / TLS Implementation Guide \[CIO-IT Security-14-69\]](#)

(18) GSA has implemented a “Bring Your Own Device (BYOD)” policy in (CIO-IT-Security-12-67) that allows users to connect their non-GSA procured smartphones and tablets, which have been previously approved by IT security, to GSA resources in a native fashion. The following IA-related guidelines outline the current BYOD Policy for GSA employees and contractors:

(a) The mobile device shall automatically lockout within 15 minutes of inactivity. The session lock shall remain in effect until the user reestablishes access using appropriate identification and authentication.

(b) The device will automatically wipe after 10 unsuccessful attempts at logon.

(c) The device will maintain a minimum passcode length of 6 characters.

b. Logical access controls.

(1) All GSA systems must implement logical access controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions.

(2) Public users must be restricted to using designated public services.

(3) Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of system users' and staff users' accounts shall be completed annually to ensure the continued need for system access.

(4) Information systems must enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Note: Detailed guidance regarding access controls is available in GSA-CIO-IT-Security-01-07: Access Control.

c. Audit records.

(1) Security-activity auditing capabilities must be employed on all GSA information systems using IT Security Procedural Guide: Auditing & Monitoring, OCIO-IT Security-01-08 and NIST SP 800-37 as guides.

(2) Audit records must be regularly reviewed/analyzed for indications of inappropriate or unusual activity. Suspicious activity or suspected violations must be investigated. Any findings must be reported to appropriate officials IAW IT Security Procedural Guide: Incident Response, OCIO-IT Security-01-02.

(3) Intrusion detection systems must be implemented as deemed appropriate by the Authorizing Official.

(4) Information systems must alert appropriate organizational officials in the event of an audit processing failure and take one of the following additional actions:

shut down information system, overwrite oldest audit records, or stop generating audit records.

(5) Information systems must produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

(6) Audit log data must be archived for a period of not less than 180 days.

(7) Systems that contain permanent electronic records must be maintained in an electronic format by 12/31/2019.

(8) All permanent and temporary e-mail records must be accessible electronically in an electronic format.

Note: Detailed guidance regarding auditing is available in GSA-CIO-IT-Security-01-08: Audit and Accountability.

d. Warning banners/system use notification message.

(1) All internal GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems. The warning banner must read as follows:

*****WARNING*****

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

(2) For publicly accessible sites (i.e., open to the Internet) the sentence, "Therefore, no expectation of privacy is to be assumed" shall be removed. Detailed guidance regarding access controls is available in GSA-CIO-IT-Security-01-07: Access Control.

e. Remote access. Access to the GSA domain must be restricted to secure methods using approved identification and authentication methods that provide detection of intrusion attempts and protection against unauthorized access.

(1) Individuals other than GSA employees and contractor personnel are not allowed to use GSA furnished computers, GSA VPN connection, or a GSA provided or funded internet connection.

(2) Users must not connect to other computers or networks via modem while simultaneously connected to the GSA network (i.e., no dialing outbound to your Internet Service Provider or allowing inbound calls to your computer while at the same time

being connected to GSA's network). However, accessing GSA's network via the GSA-provided VPN software is allowed.

(3) When using the GSA IT IPsec VPN, users must connect using only IP and must have the client firewall bound to all network adapters.

(4) Allow remote access only with multifactor authentication where one of the factors is provided by a device separate from the computer gaining access. All remote access connections shall automatically terminate within 30 minutes of inactivity.

Note: Detailed guidance regarding access controls is available in GSA-CIO-IT-Security-01-07: Access Control.

f. Vulnerability testing.

(1) GSA CIO, Service/Staff Offices, or Regions shall conduct vulnerability scanning of operating systems, information systems, databases, and web applications at least quarterly or when significant new vulnerabilities potentially affecting the system are identified and reported. All critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days IAW IT Security Procedural Guide: Managing Enterprise Risk, OCIO-IT-06-30.

(2) Independent vulnerability testing including penetration testing and system or port scanning conducted by a third party such as the GAO and other external organizations must be specifically authorized by the Authorizing Official and supervised by the ISSM.

(3) GSA S/SO/Rs shall scan for unauthorized wireless access points quarterly and take appropriate action if such an access point is discovered.

g. Encryption.

(1) All passwords must be encrypted in storage.

(2) All sensitive information, such as PII, as deemed by the Data Owner, which is transmitted outside the GSA firewall, must be encrypted. Certified encryption modules must be used IAW FIPS PUB 140-2, Security requirements for Cryptographic Modules. Your e-mail will be blocked if Social Security Numbers are sent unencrypted.

(3) When using password generated encryption keys, a password of at least 8 characters with a combination of letters, numbers, and special characters is required. A password of at least 12 characters is recommended.

(4) Systems implementing encryption must follow the key management procedures and processes documented in IT Security Procedural Guide: Key Management, OCIO-IT Security-09-43.

h. New technologies. All new technology developments, designs, and implementations shall use industry best practices, Government guidelines, and Government audit findings as they become available. Examples of new technologies include Internet Protocol v6 (IPv6) and Voice over IP (VoIP). VoIP must use NIST SP 800-58 Security considerations for Voice over IP Systems as a guide.

i. Malicious code protection. All information systems must implement and enforce a malicious code protection program designed to minimize the risk of introducing malicious code (e.g., viruses, worms, spyware, Trojan horses) into agency systems and networks.

j. Patch management. System administration and patch implementation must be restricted to authorized personnel.

k. Website privacy policy statement. Every Federal web site (internal and public) must include a privacy policy statement, even if the site does not collect any information that results in creating a Privacy Act record. Reference OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, for guidance and model language on privacy statements.

l. Account management.

(1) Request and approval routing in support of account management processes must assure:

(a) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;

(b) Users complete and send access requests to their supervisor or Contracting Officer Representative (COR), not directly to the Data or System Owner;

(c) Access requests may be aggregated and managed by designated coordinators for efficiency;

(d) Access requests are routed to the data or System Owner by a user's supervisor, COR, ISSO, ISSM, director, or designated regional coordinator.

(2) Authorizations supporting the account management processes must assure:

(a) Supervisors are responsible for coordinating and arranging system access requests for all new or transferring employees and for verifying an individual's need-to-know.

(b) Data Owners/System Owners, with assistance from the designated ISSO, ensure system access is restricted to authorized users that have completed required background investigations, are familiar with internal security practices, and

have completed requisite security and privacy awareness training programs, such as the annual Information Security & Privacy Act training curriculum. System access authorizations must enforce job function alignment, separation of duties, and be based on the principle of need-to-know. Contractors with system access must utilize a gsa.gov e-mail account to conduct business with GSA.

(3) Establishment and activations supporting the account management processes must assure:

(a) Data or System Owner grants access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.

(b) The delegation of user roles or permissions for applications, in particular those containing Personally Identifiable Information (PII) and/or sensitive financial data, must be compliant with the principles of least privilege, separation of duties, and need-to-know.

(c) Accounts are created only upon receipt of valid access requests conforming to the GSA access request protocol.

(4) Update and modification of user accounts supporting account management processes must ensure:

(a) Supervisors are responsible for coordinating and arranging system access modifications for personnel.

(b) Users complete and send account update requests directly to his or her supervisor or COR, not directly to the Data or System Owner.

(c) Update requests are aggregated and managed by designated regional coordinators for efficiency.

(d) Update requests are routed to the Data or System Owner by a user's supervisor, COR, director, or designated regional coordinator.

(5) Disabling and removal of user accounts supporting account management processes must ensure:

(a) Supervisors are responsible for coordinating and arranging system access termination for all departing or resigning personnel.

(b) Account removal is initiated by a user's supervisor, COR, or through the review of the monthly OHRM separation list submitted by the OCISO.

(c) Removal requests may be aggregated and managed by designated regional coordinators for efficiency.

(d) Termination and transfer procedures must be incorporated into the authorization process for all information systems.

(6) User authorizations must be verified annually for all information systems.

(7) User account privileges must be reviewed across the appropriate Service, Staff Office, and Region application portfolio to assess incompatible and non-compliant role assignments (e.g., review of user access assignments across multiple significant systems that share data or pass transactions to identify conflicts with separation of duties policy).

(8) On a regular basis, Data and System Owners must inspect user access entitlements as needed to detect the following conditions that warrant termination, revocation, or suspension of account access:

(a) Orphaned accounts. An orphaned account is defined as a user account that has demonstrated, or is expected to demonstrate, an extensive period of idle time consistent with account abandonment.

1. FIPS 199 Moderate and High impact systems shall automatically disable inactive accounts after 90 days and shall automatically terminate temporary and emergency accounts after no more than 90 days;

2. Upon issuance of the CISO monthly separation reports, Data and System Owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources.

(b) Role conflicts. Any accesses or permissions that clearly violate established separation of duties policies must be coordinated with the designated S/SO/R ISSO to correct or resolve conflicting role assignments.

(c) Shared accounts. Shared user accounts violate the principles of separation of duties and non-repudiation, and must be detected and suspended when discovered.

(d) Suspension or revocation of GSA e-mail accounts. Systems that require users to maintain an active e-mail account must suspend or revoke access for users whose e-mail credentials are no longer valid.

m. Trusted Internet Connection (TIC). All network devices that are either owned, managed, maintain a connection to a GSA facility, and/or handle GSA data shall be strategically positioned behind a GSA firewall to provide analysis/correlation, management structure, and minimize threats presented by external attacks. TIC will

allow GSA to provide the following security functions for any devices connected to GSA networks:

(1) Monitoring, incident response, vulnerability assessment, vulnerability management, incident reporting, engineering support, and the enforcement of the agency's specific security policy at the hosted facility.

(2) Trained, qualified, and cleared staff to; support security functions 24x7.

(3) Limited inbound and outbound connections so that only necessary services are allowed.

(4) Centralized, secured, and unified management of security events in order to protect the integrity of Government data and its infrastructure.

n. Bluetooth keyboards, mice and headsets.

(1) Bluetooth is approved for use with keyboards, mice and headsets on GSA GFE. The following restrictions apply:

(a) Devices must use the Bluetooth Protocol version 1.2 or later. If the device was manufactured 2005 or later, the version must be confirmed by consulting the device specifications.

(b) If a password/PIN must be chosen for device pairing the user should use a combination of letters and numbers when possible. A four digit pin should not be used unless this has been hardcoded by the manufacturer. Users should also use a different pass code/PIN for each pairing.

(2) The computer/device should not be discoverable except as needed for pairing. Discoverable mode (also known as "visible mode" or "pairing mode") is the mode that allows the pairing of two Bluetooth devices. Users must ensure discoverable mode is disabled after pairing is completed.

(3) Bluetooth capabilities must be disabled when they are not in use.

(a) Two devices should not remain connected for more than 23 hours at a time, since the encryption keys can repeat after this.

(b) Encryption should always be enabled for Bluetooth connections. (e.g. "Security Mode 1" does not enable encryption and therefore should never be used.)

CHAPTER 6: POLICY ON PRIVACY CONTROLS

GSA Privacy Controls provide specific guidance on security controls and privacy-related procedures used to protect GSA IT resources. According to NIST, The Privacy Controls are:

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

1. Authority and purpose.

a. **GSA Program officials must consult with the GSA Senior Agency Privacy Officer and/or Privacy Officer (SAOP/PO)** and GSA legal counsel regarding the authority of any program or activity to collect PII.

b. The authority to collect PII is documented in the System of Records Notice (SORN) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements or Computer Matching Agreements.(refer to section 3.12 above for information on Privacy Impact Assessments)

c. Personnel who handle PII must receive training on the organizational authorities for collecting PII, authorized uses of PII, and on the contents of the notice.

2. Accountability, audit, and risk management. The SAOP/PO, in consultation with legal counsel, information security officials, and others as appropriate:

a. Ensures the development, implementation, and enforcement of privacy policies and procedures;

b. Defines roles and responsibilities for protecting PII;

c. Determines the level of information sensitivity with regard to PII holdings;

d. Identifies the laws, regulations, and internal policies that apply to the PII;

e. Monitors privacy best practices; and

f. Monitors/audits compliance with identified privacy controls.

3. Data quality and integrity.

a. GSA programs authorized to collect PII must take reasonable steps to confirm the accuracy and relevance of PII. Such steps may include, editing and validating addresses as they are collected or entered into information systems using automated address verification look-up application programming interfaces (API). The types of measures taken to protect data quality are based on the nature and context of the PII, how it is to be used, and how it was obtained.

b. GSA programs must incorporate mechanisms into information systems and develop corresponding procedures for how frequently, and by what method, the information is to be updated.

4. Data minimization and retention. The GSA SAOP/PO will take appropriate steps to ensure that the collection of PII is consistent with a purpose authorized by law or regulation.

a. The minimum set of PII elements required to support a specific organization business process may be a subset of the PII the organization is authorized to collect.

b. GSA Program officials will consult with the SAOP/PO and legal counsel to identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose.

c. GSA will further reduce its privacy and security risks by also reducing its inventory of PII, where appropriate.

5. Individual participation and redress.

a. Depending upon the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII.

b. The GSA information systems may obtain consent through opt-in, opt-out, or implied consent. Opt-in consent is the preferred method, but it is not always feasible. Opt-in requires that individuals take affirmative action to allow organizations to collect or use PII. Opt-out requires individuals to take action to prevent the new or continued collection or use of such PII.

(1) Security. GSA and its agents must take due care in updating PII inventories by identifying linkable data that could create PII. 1. GSA programs may extract the following information elements from Privacy Impact Assessments (PIA) for information systems containing PII: (i) the name and acronym for each system identified; (ii) the types of PII contained in that system; (iii) classification of level of sensitivity of all types of PII, as combined in that information system; and (iv) classification of level of potential risk of substantial harm, embarrassment, inconvenience, or unfairness to affected

individuals, as well as the financial or reputational risks to organizations, if PII is exposed.

(2) Transparency.

(a) GSA must follow the process outlined in the Internal Clearance Process for GSA Data Assets policy before releasing GSA data assets. The established clearance process ensures that the privacy, security and confidentiality of our critical data assets are protected.

(b) At a minimum, GSA programs are required to:

1. Review information for valid restrictions prior to public release in order to ensure proper safeguarding of privacy, security, and confidentiality of Government proprietary and procurement sensitive information;
2. Document reasons why a data asset or certain components of a data asset should not be made public at this time;
3. Consult with the agency's Privacy Officer and general counsel regarding the barriers identified;
4. Encourage dialogue regarding resources necessary to make more data assets public.

(c) GSA programs using PII must provide an Effective Notice, which enables individuals to understand how the GSA organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to a GSA information system. The Effective notice also demonstrates the privacy considerations that the program or system has addressed in implementing its information practices. GSA may provide a general public notice facilitated through a System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy.

6. Use limitation. The GSA, by way of the SAOP/PO, will ensure the use of PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices.

- a. The PO will perform monitoring and auditing of individual program use of PII
- b. Train GSA personnel on the authorized uses of PII
- c. With guidance from the SAOP/PO and where appropriate, legal counsel, the GSA programs will document the processes and procedures for evaluating any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities.

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

March 8, 2017

Mr. Timothy O. Horne
Acting Administrator
General Services Administration
1800 F Street, N.W.
Washington, D.C. 20405

Dear Mr. Horne:

Federal recordkeeping and government transparency laws such as the Federal Records Act and the Freedom of Information Act (FOIA) ensure the official business of the government is properly preserved and accessible to the American public.¹ As the Committee with legislative jurisdiction over these laws, we have a longstanding interest in ensuring compliance with their provisions.² Over the past decade, our oversight has included monitoring trends in federal employees' use of technology in order to ensure the statutory requirements of these laws keeps pace with their original purpose. The Committee has authored several updates to these laws, such as the Presidential and Federal Records Act Amendments of 2014 and the FOIA Improvement Act of 2016.³ We plan to pursue additional efforts to update these laws.

Federal Records Act challenges have spanned across administrations. A 2013 report by the Inspector General for the Commodities Futures Trading Commission found that former Chairman Gary Gensler used his personal email consistently.⁴ Documents produced as part of the Committee's investigation into the Department of Energy's disbursement of funds under the Recovery Act showed that the former Executive Director of the Loan Program Office Jonathan Silver often used his personal email account to conduct official business.⁵

¹ Pub. L. No. 81-754 (1950); Pub. L. No. 89-487 (1967).

² See, e.g., letter from Hon. Henry Waxman, Chairman, Comm. on Oversight & Gov't Reform, to Hon. Michael Astrue, Comm'r, U.S. Soc. Sec. Admin., *et al.* (Apr. 12, 2007); letter from Hon. Darrell Issa, Chairman, Comm. on Oversight & Gov't Reform, to Hon. Jeffrey Zients, Acting Dir. for Mgmt., Office of Mgmt. & Budget, *et al.* (Dec. 13, 2012); MAJORITY STAFF OF H. COMM. ON OVERSIGHT & GOV'T REFORM, 114TH CONG., FOIA IS BROKEN: A REPORT (2016).

³ Pub. L. No. 113-187 (2014); Pub. L. No. 114-185 (2016).

⁴ OFFICE OF INSPECTOR GEN., COMMODITY FUTURES TRADING COMM'N, REVIEW OF THE COMMODITY FUTURES TRADING COMMISSION'S OVERSIGHT AND REGULATION OF MF GLOBAL, INC. (May 16, 2013).

⁵ See Carol D. Leonnig and Joe Stephens, *Energy Department loan program staffers were warned not to use personal e-mail*, WASH. POST, Aug. 14, 2012, http://articles.washingtonpost.com/2012-08-14/politics/35490043_1_personal-e-mail-e-mails-email.

Where a federal employee conducts any business related to the work of the government from a non-governmental email account, such as a personal email account, the Federal Records Act requires that the employee copy their official account or forward the record to their government email account within 20 days.⁶ Official business must be conducted in such a way as to preserve the official record of actions taken by the federal government and its employees.

Recent news reports suggest federal employees may increasingly be turning to new forms of electronic communication, including encrypted messaging applications like Signal, Confide, and WhatsApp, that could result in the creation of federal records that would be unlikely or impossible to preserve.⁷ The security of such applications is unclear.⁸ Generally, strong encryption is the best defense against cyber breaches by outside actors, and can preserve the integrity of decision-making communications. The need for data security, however, does not justify circumventing requirements established by federal recordkeeping and transparency laws.

To assist the Committee in better understanding your agency's policies on these issues, please provide the following information as soon as possible, but by no later than March 22, 2017:

1. Identify any senior agency officials who have used an alias email account to conduct official business since January 1, 2016. Include the name of the official, the alias account, and other email accounts used by the official to conduct official business.
2. Identify all agency policies referring or relating to the use of non-official electronic messaging accounts, including email, text message, messaging applications, and social media platforms to conduct official business, including but not limited to archiving and recordkeeping procedures.
3. Identify all agency policies referring or relating to the use of official text message or other messaging or communications applications, and social media platforms to conduct official business, including but not limited to archiving and recordkeeping procedures.
4. Identify agency policies and procedures currently in place to ensure all communications related to the creation or transmission of federal records on official electronic messaging accounts other than email, including social networking platforms, internal agency instant messaging systems and other communications applications, are properly captured and preserved as federal records.

⁶ 44 U.S.C. § 2911 (2017).

⁷ Andrew Restuccia, Marianne Levine, and Nahal Toosi, *Federal workers turn to encryption to thwart Trump*, POLITICO, Feb. 2, 2017, <http://www.politico.com/story/2017/02/federal-workers-signal-app-234510>; Jonathan Swan and David McCabe, *Confide: The app for paranoid Republicans*, AXIOS, Feb. 8, 2017, <https://www.axios.com/confide-the-new-app-for-paranoid-republicans-2246297664.html>.

⁸ Sheera Frenkel, *White House Staff Are Using A "Secure" App That's Not Really So Secure*, BUZZFEED NEWS, Feb. 16, 2017, <https://www.buzzfeed.com/sheerafrenkel/white-house-staff-are-using-a-secure-app-thats-really-not-so>.

Mr. Timothy O. Horne

March 8, 2017

Page 3

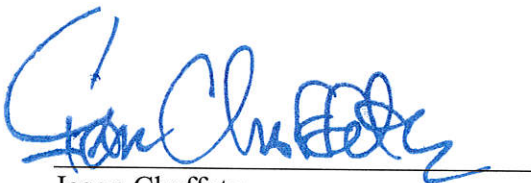
5. Explain how your agency complies with FOIA requests that may require searching and production of documents stored on non-official email accounts, social networking platforms, or other messaging or communications.
6. Provide the status of compliance by the agency with the Managing Government Records Directive issued by the Office of Management and Budget on August 24, 2012.⁹

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment to this letter provides additional information about responding to the Committee's request. Please note that Committee Rule 16(b) requires counsel representing an individual or entity before the Committee or any of its subcommittees, whether in connection with a request, subpoena, or testimony, promptly submit the attached notice of appearance to the Committee.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X.

For any questions about this request, please have your staff contact Jeff Post of the Majority staff at (202) 225-5074 or Krista Boyd of the Minority staff at (202) 225-9493. Thank you for your attention to this matter.

Sincerely,



Jason Chaffetz
Chairman



Elijah E. Cummings
Ranking Member

Enclosures

⁹ Jeffrey D. Zients, Acting Director, Office of Management and Budget and David S. Ferriero, Archivist of the United States, National Archives and Records Administration, *Managing Government Records Directive* (Aug. 24, 2012) (M-12-18).

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
 - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
 - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,
CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE,
DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,
INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.
6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.
17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.

19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.
3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term “referring or relating,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term “employee” means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.

**COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
115TH CONGRESS**

NOTICE OF APPEARANCE OF COUNSEL

Counsel submitting: _____

Bar number: _____ **State/District of admission:** _____

Attorney for: _____

Address: _____

Telephone: (_____) _____ - _____

Pursuant to Rule 16 of the Committee Rules, notice is hereby given of the entry of the undersigned as counsel for _____ in (select one):

All matters before the Committee

The following matters (describe the scope of representation):

All further notice and copies of papers and other material relevant to this action should be directed to and served upon:

Attorney's name: _____

Attorney's email address: _____

Firm name (where applicable): _____

Complete Mailing Address: _____

I agree to notify the Committee within 1 business day of any change in representation.

Signature of Attorney

Date



June 29, 2017

The Honorable Ben Cardin
Ranking Member
Subcommittee on Transportation
and Infrastructure
Committee on Environment
and Public Works
United States Senate
Washington, DC 20510

Dear Senator Cardin:

Thank you for your letter dated April 6, 2017, regarding the U. S. General Services Administration's (GSA) policy for responding to congressional oversight inquiries.

As Acting Administrator Timothy O. Horne discussed during your April 26, 2017, meeting, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed *Letter Opinion for the Counsel to the President*. In this Letter, the U.S. Department of Justice Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each house of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the executive branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III", with a stylized, cursive script.

P. Brennan Hart III
Associate Administrator

Enclosure

Congress of the United States

Washington, DC 20515

April 6, 2017

Mr. Timothy Horne
Acting Administrator
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Acting Administrator Horne:

We understand that, as of January 20, 2017, the General Services Administration (GSA) no longer feels obligated to respond to requests for information by Ranking Members of the Congressional committees with legislative and oversight jurisdiction over your agency and its programs. This partisan change in policy is unacceptable.

Under the Obama administration, the GSA Administrator responded to requests for information from Ranking Members of such Congressional committees regardless of whether the Ranking Member was a Democrat or a Republican. Under the Trump administration, the GSA policy appears to be to respond to Republican Chairmen but not Democratic Ranking Members. It has not gone unnoticed that your agency has been nonresponsive to our inquiries since that time.

We regard this as a serious breach of protocol and an abdication of your responsibility to run an open and transparent independent agency on behalf of the American people. GSA's mission to provide billions of dollars in procurement services for Federal agencies carries with it the obligation to ensure that taxpayers are getting the best value possible for their hard-earned tax dollars. This mandate requires that your agency spend wisely, upholding the highest ethical standards. It also requires that your agency disclose information about its policies and the decisions it makes to us, the elected representatives of the American people.

We expect a prompt reply that includes answers to all of our previous inquiries, as well as answers to the following questions:

1. Is it now the policy of GSA that it may decline to provide information requested by Ranking Members of Congressional committees of jurisdiction? How does this policy differ from the policy of the Obama administration?
2. When was the most recent directive on this matter issued, in any form, to GSA staff? Who issued that directive and what was the content? If the directive was in writing or in electronic format, please provide us with a copy.
3. Did the White House or any other Federal agency provide GSA with advice or instruction on this matter?

Mr. Timothy Horne
April 6, 2017
Page 2

We strongly urge you to immediately rescind this partisan policy and provide the information we require so that our Committees can conduct oversight of the agency. Please respond in writing to this letter no later than April 13, 2017.

Sincerely,



PETER DeFAZIO
Ranking Member
Committee on Transportation
and Infrastructure
United States House of Representatives



TOM CARPER
Ranking Member
Committee on Environment
and Public Works
United States Senate



HANK JOHNSON
Ranking Member
Subcommittee on Economic Development,
Public Buildings, and Emergency
Management
United States House of Representatives



BEN CARDIN
Ranking Member
Subcommittee on Transportation
and Infrastructure
United States Senate

cc: The Honorable Bill Shuster
Chairman, Committee on Transportation and Infrastructure

The Honorable John Barrasso
Chairman, Committee on Environment and Public Works

The Honorable Lou Barletta
Chairman, Subcommittee on Economic Development, Public Buildings and Emergency
Management

The Honorable James Inhofe
Chairman, Subcommittee on Transportation and Infrastructure

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051
<http://oversight.house.gov>

June 5, 2017

Timothy O. Horne
Acting Administrator
General Services Administration
1800 F Street, NW
Washington, D.C. 20405

Dear Acting Administrator Horne:

We are writing to renew a request we sent to the General Services Administration (GSA) on February 8, 2017, pursuant to the statutory “Seven Member Rule,” to obtain complete, unredacted copies of documents related to the administration of the Old Post Office lease agreement with President Donald Trump’s company.

Background on Statutory Seven Member Rule

Last week, the Trump Administration released an opinion issued by the Office of Legal Counsel on May 1, 2017, arguing that agencies and departments could ignore requests for documents and other information from Members of Congress other than Republican Committee Chairmen. The opinion asserted:

[T]he constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of executive branch programs and activities—may be exercised only by each house of Congress or, under existing delegations, by committee and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.¹

This opinion is flawed in many ways, but even taking it at face value, GSA must comply with requests submitted under the statutory Seven Member Rule. The Seven Member Rule is unique authority that was passed by both the House and Senate and signed by the President in 1928, explicitly delegating authority for any seven members of the Committee on Oversight and Government Reform to require any executive agency to “submit any information requested of it

¹ Office of Legal Counsel, Department of Justice, *Authority of Individual Members of Congress to Conduct Oversight of the Executive Branch* (May 1, 2017) (online at www.justice.gov/olc/file/966326/download).

relating to any matter within the jurisdiction of the committee.”²

Under House Rule X, the Committee has jurisdiction over “Government management and accounting measures generally,” as well as the “Overall economy, efficiency, and management of government operations and activities, including Federal procurement.”³ In addition, as the primary investigative body in the House, the Committee also has the broad authority “at any time” to “conduct investigations” of “any matter.”⁴

For example, in *Henry A. Waxman v. Donald L. Evans*, United States District Court Judge Lourdes G. Baird granted 16 members of the Committee summary judgment in a case brought against the Department of Commerce to enforce the Seven Member Rule. The court ruled that the Department was required to provide adjusted data from the 2000 census.⁵

Compliance with Seven Member Rule Under Obama Administration

During the Obama Administration, GSA explicitly recognized and complied with a request for documents under the statutory Seven Member Rule regarding the Old Post Office lease agreement. On December 22, 2016, 11 members of the Committee sent GSA a request for documents pursuant to the Seven Member Rule.⁶ In response, GSA produced documents on January 3, 2017, writing:

Thank you for your letter dated December 22, 2016, from 11 members of the House Committee on Oversight and Government Reform requesting certain records related to the Old Post Office pursuant to 5 U.S.C. § 2954 (the “Seven Member Rule”). ... Consistent with the Seven Member Rule and judicial and Department of Justice, Office of Legal Counsel opinions (see e.g., 6 Op. O.L.C. 632 (1982) and 28 Op. O.L.C. 79 (2004)), enclosed please find attachments responsive to your request.⁷

² 5 U.S.C. § 2954 (incorporating and amending 45 Stat. 996 (1928)). The statutory language refers to the “Committee on Government Operations.” The Committee was renamed several times since then, and in the 110th Congress, it was renamed the Committee on Oversight and Government Reform. References in statute to the “Committee on Government Operations” are treated as referring to the Committee on Oversight and Government Reform.

³ House rule X, clause 1(n).

⁴ House rule X, clause 4(c)(2).

⁵ *Henry A. Waxman v. Donald L. Evans*, CV 01-4530 LGB (AJWx), 2002 U.S. Dist. LEXIS 25975, at *33 (C.D. Cal. Jan. 18, 2002).

⁶ Letter from Ranking Member Elijah E. Cummings, et al., House Committee on Oversight and Government Reform, to Denise Turner Roth, Administrator, General Services Administration (Dec. 22, 2016) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2016-12-22.EEC%20et%20al%20to%20Roth%20re%20Trump%20International%20Hotel.pdf>).

⁷ Letter from Lisa A. Austin, Associate Administrator, General Services Administration, to Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform (Jan. 3, 2017) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/GSA%20Response%20to%20Seven%20Member%20Rule%2001-03-17.pdf>).

GSA produced a wide range of documents—in unredacted form—including an amendment to the lease, a 2017 budget estimate, exhibits to the lease, and monthly income statements for the Trump International Hotel.

Similarly, during the Obama Administration, the State Department also complied with a request submitted by Members of our Committee under the Seven Member Rule. On September 2, 2016, 11 Members of the Committee sent a letter pursuant to the Seven Member Rule, requesting an unredacted copy of an email exchange between former Secretary of State Colin Powell and former Secretary of State Hillary Clinton.⁸ On September 7, 2017, the State Department produced the full, unredacted email exchange in response to the request.⁹

Failure to Comply with Seven Member Rule Under Trump Administration

During the Trump Administration, GSA has recognized the existence of the Seven Member Rule, but has failed to comply with it to date.

On January 23, 2017, Ranking Members Cummings, DeFazio, Connolly, and Carson sent a letter requesting documents relating to the Old Post Office lease.¹⁰ In declining to provide these documents to the Ranking Members alone, GSA sent a response on February 6, 2017, acknowledging the authority of Committee Members to obtain information under the Seven Member Rule. Acting Associate Administrator Saul Japson wrote:

GSA is unable to provide the unredacted versions of the monthly reports describing revenue and expenses. Should the U.S. House of Representatives Committee on Oversight and Government Reform or any seven members thereof submit a request pursuant to 5 U.S.C. § 2954, GSA will review any such request.¹¹

⁸ Letter from Ranking Member Elijah E. Cummings, et al., House Committee on Oversight and Government Reform, to Secretary of State John F. Kerry, Department of State (Sept. 2, 2016) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2016-09-02.%20OGR%20dem%20members%20to%20Kerry.pdf>).

⁹ Letter from Julia Frifield, Assistant Secretary for Legislative Affairs, Department of State, to Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform (Sept. 7, 2016) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/State%20to%20EEC%2009-07-16.pdf>).

¹⁰ Letter from Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform, Ranking Member Peter A. DeFazio, House Committee on Transportation and Infrastructure, Rep. Gerald Connolly, and Rep. André Carson, to Timothy Horne, Acting Administrator, General Services Administration (Jan. 23, 2017) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2017-01-23.EEC%2C%20DeFazio%2C%20Connolly%2C%20%26%20Carson%20to%20GSA%20OPO%20Letter%20re.%20Trump.pdf>).

¹¹ Letter from Acting Associate Administrator Saul Japson, General Services Administration, to Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform (Feb. 6, 2017) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/GSA%20letter.pdf>).

Following this suggestion, two days later, on February 8, 2017, eight members of the Committee sent a letter to GSA requesting these documents pursuant to the statutory Seven Member Rule.¹² Over the past four months, our staffs have inquired repeatedly about the status of this request, but we have received no further response from GSA.

Instead, you testified on May 24, 2017, before the House Committee on Appropriations that the Trump Administration's new policy—to reject all oversight requests from Democrats unless they are also joined by Republican Committee Chairmen—could preclude the production of documents under the Seven Member Rule. In response to questions from Rep. Matt Cartwright, who is also a Member of the Oversight Committee, you testified: “the Administration has instituted a new policy that matters of oversight need to be requested by the Committee chair.” You also testified that you would respond to Democratic requests by providing only public information with other information redacted:

However, if it's an oversight matter, not requested by the Committee chair, we'll respond with a letter saying that—you know, if it's information that we need to be redacted, then we will redact the information—we will provide public information. But for matters of oversight, the request needs to come from the Committee chair.¹³

Request for Documents Under Statutory Seven Member Rule

The Seven Member Rule is not a regulation or guideline, but a statute that was passed by both houses of Congress and signed by the President. Although you may wish to limit oversight from Democratic Members of Congress through a misguided policy that responds only to Republican Chairmen, compliance with federal law is not an optional exercise that may be overridden by a new Trump Administration policy.

Your actions to date are not only a reversal of previous Executive Branch policy and a direct impediment to authorized congressional oversight, but a violation of the statute passed by Congress creating the Seven Member Rule and explicitly delegating this authority to Members of the Oversight Committee. For these reasons, we request, pursuant to the Seven Member Rule, that you produce the following documents—in unredacted form—by June 23, 2017:

1. all monthly reports submitted to GSA since November 2016 by Trump Old Post Office LLC describing revenues and expenses;
2. all correspondence and documents from Trump Old Post Office LLC relating to liens or any action to resolve liens;

¹² Letter from Ranking Member Elijah E. Cummings, et al., House Committee on Oversight and Government Reform, to Saul Japson, Acting Associate Administrator, General Services Administration (Feb. 8, 2017) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2017-02-08.EEC%20et%20al%20to%20Japson-GSA%20re%20Trump%20International%20Hotel.pdf>).

¹³ House Committee on Appropriations, Subcommittee on Financial Services and General Government, *Hearing on the General Services Administration*, 115th Cong. (May 24, 2017).

3. all correspondence with representatives of Trump Old Post Office LLC, the Trump transition team, or the Trump Administration regarding compliance with the lease before or after the presidential election, Section 37.19 of the lease, the monthly financial reports, the structure of the trust created to address Section 37.19 of the lease, or any other matters above;
4. all correspondence and documents relating to funds received from any foreign country, foreign entity, or foreign source;
5. correspondence from Adam L. Rosen on December 16, 2016, and December 29, 2016, to GSA, referenced in the attachment to GSA's February 6, 2017, letter to Members of this Committee;
6. all correspondence and documents relating to representatives of the tenant in its interactions with GSA;
7. all documents containing legal interpretations of Section 37.19 of the lease created within GSA or received from the tenant;
8. any legal opinion relied upon by GSA in making a determination regarding the President's compliance with Section 37.19; and
9. all drafts and edits of Kevin Terry's letter on March 23, 2017, including who authored the drafts or edits.

Thank you for your prompt cooperation with this matter.

Sincerely,

Elijah E. Cummings

Wesley B. Denning

MARK DE

Brenda Laurence

Jamie Raskin

Stacey E. Plaskett

Matthew A. Cartwright

Rubin Kelly

Bonnie Watson-Coleman

Eleanor H. Norton

Ann E. Quinn

Cordye B. Malore

Wm. Lucy Gray

John

Raja K. Kulkarni

Steph J. Lynch

Peter Welch

John P. Larkin

cc: The Honorable Jason Chaffetz, Chairman



The Administrator

June 7, 2017

The Honorable Rodney Frelinghuysen
The Honorable Nita Lowey
Chairman and Ranking Member
Committee on Appropriations
House of Representatives
Washington, DC 20515

The Honorable Thad Cochran
The Honorable Patrick Leahy
Chairman and Ranking Member
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Tom Graves
The Honorable Mike Quigley
Chairman and Ranking Member
Subcommittee on Financial Services
and General Government
Committee on Appropriations
House of Representatives
Washington, DC 20515

The Honorable Shelley Moore Capito
The Honorable Christopher Coons
Chairman and Ranking Member
Subcommittee on Financial Services
and General Government
United States Senate
Washington, DC 20510

Dear Chairmen and Ranking Members:

The purpose of this letter is to provide information about planned organizational changes at the U.S. General Service Administration (GSA), consistent with Section 608 of the Consolidated Appropriations Act, 2017 (P.L. 115-31).

1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

In line with GSA's mission to provide the best value in technology services to the government and the American people, GSA plans to implement a reorganization of the Technology Transformation Service (TTS). Under the reorganization, GSA will transfer all offices, personnel, and functions within the TTS to the established Technology Transformation Services under the Federal Acquisition Service (FAS). A new position of Deputy Commissioner reporting to the Commissioner of FAS will head the Technology Transformation Services.

This reorganization will promote the growth and long-term viability of the Technology Transformation Services by providing it with access to the authorities, funding and structure within FAS, a mature organization, which are critical to the office accomplishing its mission of transforming government technology. This reorganization will also allow GSA to eliminate duplicative functions within FAS and TTS that will result in streamlined government operations, and thus, will lead to saving taxpayer money.

GSA is committed to being a leading force in the campaign to modernize the federal government. That means transforming how we work to be more agile and cost effective and provide better service for our agency partners and the American people.

I have enclosed a copy of the draft GSA Order which provides information on the offices and functions that will be impacted by this change. Should you have any questions or concerns, please do not hesitate to contact me at (202) 501-0800 or Brennan Hart, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

(b) (6)

Timothy Horne
Acting Administrator

Enclosure

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

ADM 5440.7##
Insert Date

GSA ORDER

Subject: Change in GSA Organization – Federal Acquisition Service and Technology Transformation Service

1. Purpose. This order outlines the organizational and reporting structure of the U.S. General Services Administration (GSA), Technology Transformation Service (TTS) and the Federal Acquisition Service (FAS).
2. Cancellation. ADM 5440.696 dated April 29, 2016, ADM 5440.700 dated July 21, 2016, ADM 5440.709 dated October 11, 2016, and TTS 5440.1 dated March 16, 2017.
3. Background. ADM 5440.696 announced the establishment of TTS and the establishment of the Commissioner of TTS. ADM 5440.700 delineated the organizational structure of TTS. ADM 5440.709 and TTS 5440.1 made additional refinements to TTS and the organizational structure of the Office of 18F. A decision has been made to transfer the existing TTS organization under FAS.
4. Changes in organization.
 - a. The Technology Transformation Services is established under FAS. The organization is headed by an individual who serves as Deputy Commissioner and Director of Technology Transformation Services, reporting to the Commissioner of FAS and has a direct line of engagement with the Administrator on a recurring basis.
 - b. The Technology Transformation Service is transferred to Technology Transformation Services, FAS. The offices included in this move include those below. Each is headed by an Assistant Commissioner who reports to the Deputy Commissioner/ Director of Technology Transformation Services.
 1. The Office of Presidential Innovation Fellows;
 2. The Office of 18F;
 3. The Office of Operations;
 4. The Office of Products and Programs; and
 5. The Office of Acquisition.

5. Implementing actions.

- a. The changes outlined in this Order become effective upon signature. Implementation of this Order will be coordinated between the affected organizations, in consultation with the Chief Human Capital Officer (CHCO) and the Chief Financial Officer (CFO), to ensure the appropriate alignment of the functions, staff, authorities, and other resources associated with the changes outlined above in paragraph 4.
- b. Implementation of this Order, as it affects employees represented by a labor bargaining unit, is contingent upon completion of labor relations obligations. Positions affected by this change are subject to normal classification procedures.
- c. The approval of this Order authorizes the determination and appropriate adjustments including realignment among offices of budget and funding sources as determined by the CFO.
- d. The Chief Administrative Officer may cancel this Order, in consultation with the CHCO, upon publication of a superseding directive that cancels it in accordance with OAS P 1832.1A.

5. Signature.

TIMOTHY HORNE
Acting Administrator

DATE



The Administrator

June 7, 2017

The Honorable Rodney Frelinghuysen
The Honorable Nita Lowey
Chairman and Ranking Member
Committee on Appropriations
House of Representatives
Washington, DC 20515

The Honorable Thad Cochran
The Honorable Patrick Leahy
Chairman and Ranking Member
Committee on Appropriations
United States Senate
Washington, DC 20510

The Honorable Tom Graves
The Honorable Mike Quigley
Chairman and Ranking Member
Subcommittee on Financial Services
and General Government
Committee on Appropriations
House of Representatives
Washington, DC 20515

The Honorable Shelley Moore Capito
The Honorable Christopher Coons
Chairman and Ranking Member
Subcommittee on Financial Services
and General Government
United States Senate
Washington, DC 20510

Dear Chairmen and Ranking Members:

The purpose of this letter is to provide information about planned organizational changes at the U.S. General Service Administration (GSA), consistent with Section 608 of the Consolidated Appropriations Act, 2017 (P.L. 115-31).

1800 F Street, NW
Washington, DC 20405-0002

www.gsa.gov

In line with GSA's mission to provide the best value in technology services to the government and the American people, GSA plans to implement a reorganization of the Technology Transformation Service (TTS). Under the reorganization, GSA will transfer all offices, personnel, and functions within the TTS to the established Technology Transformation Services under the Federal Acquisition Service (FAS). A new position of Deputy Commissioner reporting to the Commissioner of FAS will head the Technology Transformation Services.

This reorganization will promote the growth and long-term viability of the Technology Transformation Services by providing it with access to the authorities, funding and structure within FAS, a mature organization, which are critical to the office accomplishing its mission of transforming government technology. This reorganization will also allow GSA to eliminate duplicative functions within FAS and TTS that will result in streamlined government operations, and thus, will lead to saving taxpayer money.

GSA is committed to being a leading force in the campaign to modernize the federal government. That means transforming how we work to be more agile and cost effective and provide better service for our agency partners and the American people.

I have enclosed a copy of the draft GSA Order which provides information on the offices and functions that will be impacted by this change. Should you have any questions or concerns, please do not hesitate to contact me at (202) 501-0800 or Brennan Hart, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-0563.

Sincerely,

(b) (6)

Timothy Horne
Acting Administrator

Enclosure

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

ADM 5440.7##
Insert Date

GSA ORDER

Subject: Change in GSA Organization – Federal Acquisition Service and Technology Transformation Service

1. Purpose. This order outlines the organizational and reporting structure of the U.S. General Services Administration (GSA), Technology Transformation Service (TTS) and the Federal Acquisition Service (FAS).
2. Cancellation. ADM 5440.696 dated April 29, 2016, ADM 5440.700 dated July 21, 2016, ADM 5440.709 dated October 11, 2016, and TTS 5440.1 dated March 16, 2017.
3. Background. ADM 5440.696 announced the establishment of TTS and the establishment of the Commissioner of TTS. ADM 5440.700 delineated the organizational structure of TTS. ADM 5440.709 and TTS 5440.1 made additional refinements to TTS and the organizational structure of the Office of 18F. A decision has been made to transfer the existing TTS organization under FAS.
4. Changes in organization.
 - a. The Technology Transformation Services is established under FAS. The organization is headed by an individual who serves as Deputy Commissioner and Director of Technology Transformation Services, reporting to the Commissioner of FAS and has a direct line of engagement with the Administrator on a recurring basis.
 - b. The Technology Transformation Service is transferred to Technology Transformation Services, FAS. The offices included in this move include those below. Each is headed by an Assistant Commissioner who reports to the Deputy Commissioner/ Director of Technology Transformation Services.
 1. The Office of Presidential Innovation Fellows;
 2. The Office of 18F;
 3. The Office of Operations;
 4. The Office of Products and Programs; and
 5. The Office of Acquisition.

5. Implementing actions.

- a. The changes outlined in this Order become effective upon signature. Implementation of this Order will be coordinated between the affected organizations, in consultation with the Chief Human Capital Officer (CHCO) and the Chief Financial Officer (CFO), to ensure the appropriate alignment of the functions, staff, authorities, and other resources associated with the changes outlined above in paragraph 4.
- b. Implementation of this Order, as it affects employees represented by a labor bargaining unit, is contingent upon completion of labor relations obligations. Positions affected by this change are subject to normal classification procedures.
- c. The approval of this Order authorizes the determination and appropriate adjustments including realignment among offices of budget and funding sources as determined by the CFO.
- d. The Chief Administrative Officer may cancel this Order, in consultation with the CHCO, upon publication of a superseding directive that cancels it in accordance with OAS P 1832.1A.

5. Signature.

TIMOTHY HORNE
Acting Administrator

DATE



Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

Mathew M. Sturges, Staff Director

Katherine W. Dedrick, Democratic Staff Director

June 13, 2017

Mr. Timothy Horne
Acting Administrator
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Acting Administrator Horne:

As Ranking Members of the House Committee and Subcommittee with jurisdiction over the General Services Administration (GSA) Public Building Service, we have repeatedly written to you seeking information essential to our constitutional oversight duties. You have failed to respond substantively to multiple requests for information. Your failure to respond is unacceptable.

On January 23, 2017, Ranking Member DeFazio, together with Committee on Oversight and Government Reform Ranking Member Cummings, wrote to you asking you to re-evaluate the Old Post Office lease agreement between GSA and the Trump Old Post Office, LLC. Specifically, we requested that you evaluate the Old Post Office lease agreement in light of the announcement by President-elect Donald Trump on January 11 that he was refusing to divest his ownership interests in the Trump Old Post Office, LLC; and that on January 20, 2017, he took the oath of office to become the 45th President of the United States, creating the untenable position of being both landlord and tenant of the Old Post Office building.

In that same letter, we also asked you to explain the steps that GSA had taken or planned to take to address President Trump's apparent breach of the Old Post Office lease agreement provision barring any elected official from being a lessee, or deriving any benefit from the lease. We asked GSA for copies of any notices sent to Trump Old Post Office, LLC concerning the breach of lease or notices sent in response to the public reports of construction liens filed against the Old Post Office building. In addition, we requested unredacted monthly reports of both the revenues and expenses for the Trump International Hotel and any correspondence that GSA had with Trump Old Post Office, LLC or the Trump transition team regarding the Trump International Hotel.

In a response letter of February 6, 2017, your then-Acting Associate Administrator declined to provide any of the substantive information that we requested. He explicitly stated that GSA would not provide the unredacted revenue and expense reports. Further, he stated that GSA was "monitoring" the issue of mechanics' liens against the Hotel, but provided no other information.

Mr. Timothy Horne

June 13, 2017

Page 2

Finally, he provided copies of two letters from GSA to Trump Old Post Office, LLC, yet the text of these letters clearly indicates there exists additional material responsive to our request that was not provided.

On March 23, 2017, the GSA contracting officer for the Old Post Office lease agreement wrote to Donald Trump, Jr., that the Trump Old Post Office, LLC was in full compliance with the lease (the aforementioned deficiencies notwithstanding). Given the intense Congressional interest in this matter, GSA held an in-person briefing that provided answers to some of our questions, though most of our inquiries were not addressed. Specifically, GSA continued to refuse to provide the monthly reports required by the lease agreement, making it impossible to understand the financial health of the Trump International Hotel at the Old Post Office, whether there are Foreign Emoluments clause violations, whether the Trump Old Post Office, LLC is meeting its financial goals, and whether GSA is receiving its share of profits pursuant to the Old Post Office lease agreement.

Of note, at that briefing, the Deputy Commissioner of the Public Buildings Service stated that on January 20, 2017, GSA policy regarding providing information to Congress changed. He stated that GSA will respond to requests by Ranking Members on a discretionary basis only, and that GSA no longer considered an inquiry from a Committee Ranking Member to require a response.

On April 6, 2017, together with Committee on Environment and Public Works Ranking Member Carper and Subcommittee on Transportation and Infrastructure Cardin of the Senate, we wrote to you demanding an explanation of why information requested by Ranking Members has not been provided by GSA. The letter requested an explanation for this partisan change in policy, which officials provided this guidance, and whether the White House or any other federal agency provided instruction on this matter. We have not yet received an answer to this inquiry.

Under the Trump administration, GSA has been nonresponsive to our written inquiries. We regard this as an abdication of your responsibility to run an open and transparent independent agency on behalf of the American people. GSA's mission to provide billions of dollars in real estate services for Federal agencies carries with it the obligation to ensure that taxpayers are getting the best value possible in every lease agreement. This mandate requires your agency to disclose information about its policies and the decisions it makes to us, the elected representatives of the American people.

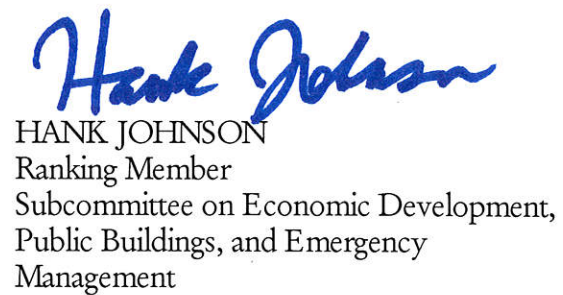
We strongly urge you to respond to our previous letters by June 19, 2017, and provide the information we require so that our Committee can fulfill its constitutional duty to conduct oversight of GSA.

Mr. Timothy Horne
June 13, 2017
Page 3

Sincerely,



PETER DeFAZIO
Ranking Member



HANK JOHNSON
Ranking Member
Subcommittee on Economic Development,
Public Buildings, and Emergency
Management

cc: The Honorable Bill Shuster
Chairman, Committee on Transportation and Infrastructure

The Honorable Lou Barletta
Chairman, Subcommittee on Economic Development, Public Buildings, and Emergency
Management



June 29, 2017

The Honorable Peter DeFazio
Ranking Member
Committee on Transportation
and Infrastructure
House of Representatives
Washington, DC 20515

Dear Representative DeFazio:

Thank you for your letters to Acting Administrator Timothy O. Horne dated April 6, 2017, and June 13, 2017, regarding the lease agreement for the Old Post Office (OPO) building in Washington, DC, and the U.S. General Services Administration's (GSA) policy regarding congressional oversight requests. Your inquiries have been referred to me for response.

As noted in your correspondence, GSA responded to previous requests for information pertaining to the OPO building lease. GSA also provided briefings on this matter to your staff on December 8, 2016, and March 31, 2017. Additionally, on March 23, 2017, GSA provided the Contracting Officer's decision and accompanying documents to your staff. During the March 31 briefing, GSA addressed the issues raised in your correspondence, including the lease procurement process, the terms of the lease, the tenant's organizational structure, and GSA's Contracting Officer's determination that the tenant is in full compliance with Section 37.19, and that the lease is valid and in full force and effect.

Per subsection 1.602-1 of the Federal Acquisition Regulation, "Contracting officers have authority to enter into, administer, or terminate contracts and make related determinations and findings." GSA's responsibility is to ensure that terms and conditions of the lease GSA signed are fully enforced. With regard to your concerns about conflicts of interest and constitutional matters, as GSA indicated in briefings to your staff and prior correspondence, it is the responsibility of other Federal entities, including the Office of Government Ethics, the U.S. Department of Justice's Office of Legal Counsel, and the White House Counsel to evaluate those issues.

For more information on the terms and conditions of the lease, and for related documentation and communications between GSA and various organizations and entities, please visit www.gsa.gov/portal/content/305477.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed *Letter Opinion for the Counsel to the President*. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen).

Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

A similar letter has been sent to your colleague. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,



P. Brennan Hart III
Associate Administrator

Enclosure



June 29, 2017

The Honorable Hank Johnson
Ranking Member
Subcommittee on Economic Development,
Public Buildings, and Emergency Management
Committee on Transportation
and Infrastructure
House of Representatives
Washington, DC 20515

Dear Representative Johnson:

Thank you for your letters to Acting Administrator Timothy O. Horne dated April 6, 2017, and June 13, 2017, regarding the lease agreement for the Old Post Office (OPO) building in Washington, DC, and the U.S. General Services Administration's (GSA) policy regarding congressional oversight requests. Your inquiries have been referred to me for response.

As noted in your correspondence, GSA responded to previous requests for information pertaining to the OPO building lease. GSA also provided briefings on this matter to your staff on December 8, 2016, and March 31, 2017. Additionally, on March 23, 2017, GSA provided the Contracting Officer's decision and accompanying documents to your staff. During the March 31 briefing, GSA addressed the issues raised in your correspondence, including the lease procurement process, the terms of the lease, the tenant's organizational structure, and GSA's Contracting Officer's determination that the tenant is in full compliance with Section 37.19, and that the lease is valid and in full force and effect.

Per subsection 1.602-1 of the Federal Acquisition Regulation, "Contracting officers have authority to enter into, administer, or terminate contracts and make related determinations and findings." GSA's responsibility is to ensure that terms and conditions of the lease GSA signed are fully enforced. With regard to your concerns about conflicts of interest and constitutional matters, as GSA indicated in briefings to your staff and prior correspondence, it is the responsibility of other Federal entities, including the Office of Government Ethics, the U.S. Department of Justice's Office of Legal Counsel, and the White House Counsel to evaluate those issues.

For more information on the terms and conditions of the lease, and for related

1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

documentation and communications between GSA and various organizations and entities, please visit www.gsa.gov/portal/content/305477.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen).

Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

A similar letter has been sent to your colleague. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,



P. Brennan Hart III
Associate Administrator

Enclosure

Authority of Individual Members of Congress to Conduct Oversight of the Executive Branch

The constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of executive branch programs and activities—may be exercised only by each house of Congress or, under existing delegations, by committees and subcommittees (or their chairmen).

Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee. They may request information from the Executive Branch, which may respond at its discretion, but such requests do not trigger any obligation to accommodate congressional needs and are not legally enforceable through a subpoena or contempt proceedings.

May 1, 2017

LETTER OPINION FOR THE COUNSEL TO THE PRESIDENT

We understand that questions have been raised about the authority of individual members of Congress to conduct oversight of the Executive Branch. As briefly explained below, the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of executive branch programs and activities—may be exercised only by each house of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee. Accordingly, the Executive Branch’s longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

The Constitution vests “[a]ll legislative Powers” in “a Congress of the United States, which shall consist of a Senate and House of Representatives.” U.S. Const. art. I, § 1. The Supreme Court has recognized that one of those legislative powers is the implicit authority of each house of Congress to gather information in aid of its legislative function. *See McGrain v. Daugherty*, 273 U.S. 135, 174 (1927). Each house may exercise its authority directly—for example, by passing a resolution of inquiry seeking information from the Executive Branch. *See 4 Deschler’s Precedents of the United States House of Representatives*, ch. 15, § 2, at 30–50

(1981) (describing the practice of resolutions of inquiry and providing examples); Floyd M. Riddick & Alan S. Frumin, *Riddick's Senate Procedure*, S. Doc. No. 101-28, at 882 (1992) (“The Senate itself could investigate or hear witnesses as it has on rare occasions[.]”).

In modern practice, however, each house typically conducts oversight “through delegations of authority to its committees, which act either through requests by the committee chairman, speaking on behalf of the committee, or through some other action by the committee itself.” *Application of Privacy Act Congressional-Disclosure Exception to Disclosures to Ranking Minority Members*, 25 Op. O.L.C. 289, 289 (2001) (“*Application of Privacy Act*”); see also Alissa M. Dolan et al., Cong. Research Serv., RL30240, *Congressional Oversight Manual* 65 (Dec. 19, 2014). As the Supreme Court has explained, “[t]he theory of a committee inquiry is that the committee members are serving as the representatives of the parent assembly in collecting information for a legislative purpose” and, in such circumstances, “committees and subcommittees, sometimes one Congressman, are endowed with the full power of the Congress to compel testimony.” *Watkins v. United States*, 354 U.S. 178, 200–01 (1957).

By contrast, individual members, including ranking minority members, “generally do not act on behalf of congressional committees.” *Application of Privacy Act*, 25 Op. O.L.C. at 289; see also *id.* at 289–90 (concluding that “the Privacy Act’s congressional-disclosure exception does not generally apply to disclosures to ranking minority members,” because ranking minority members “are not authorized to make committee requests, act as the official recipient of information for a committee, or otherwise act on behalf of a committee”). Under existing congressional rules, those members have not been “endowed with the full power of the Congress” (*Watkins*, 354 U.S. at 201) to conduct oversight. See *Congressional Oversight Manual* at 65; see also *Exxon Corp. v. FTC*, 589 F.2d 582, 593 (D.C. Cir. 1978) (“[D]isclosure of information can only be compelled by authority of Congress, its committees or subcommittees, not solely by individual members; and only for investigations and congressional activities.”). Individual members who have not been authorized to conduct oversight are entitled to no more than “the *voluntary* cooperation of agency officials or private persons.” *Congressional Oversight Manual* at 65 (emphasis added).

The foregoing reflects the fundamental distinction between constitutionally authorized oversight and other congressional requests for infor-

mation. When a committee, subcommittee, or chairman exercising delegated oversight authority asks for information from the Executive Branch, that request triggers the “implicit constitutional mandate to seek optimal accommodation . . . of the needs of the conflicting branches.” *United States v. AT&T Co.*, 567 F.2d 121, 127 (D.C. Cir. 1977); *see also id.* at 130–131 (describing the “[n]egotiation between the two branches” as “a dynamic process affirmatively furthering the constitutional scheme”). Such oversight requests are enforceable by the issuance of a subpoena and the potential for contempt-of-Congress proceedings. *See McGrain*, 273 U.S. at 174; 2 U.S.C. §§ 192, 194; *see also* Standing Rules of the Senate, Rule XXVI(1), S. Doc. No. 113-18, at 31 (2013) (empowering all standing committees to issue subpoenas); Rules of the House of Representatives, 115th Cong., Rule XI, cl. 2(m)(1) (2017) (same). Upon receipt of a properly authorized oversight request, the Executive Branch’s longstanding policy has been to engage in the accommodation process by supplying the requested information “to the fullest extent consistent with the constitutional and statutory obligations of the Executive Branch.” Memorandum for the Heads of Executive Departments and Agencies from President Ronald Reagan, *Re: Procedures Governing Responses to Congressional Requests for Information* (Nov. 4, 1982). But a letter or inquiry from a member or members of Congress not authorized to conduct oversight is not properly considered an “oversight” request. *See Congressional Oversight Manual* at 56 (“Individual Members, Members not on a committee of jurisdiction, or minority Members of a jurisdictional committee, may, like any person, request agency records. When they do, however, they are not acting pursuant to Congress’s constitutional authority to conduct oversight and investigations.”). It does not trigger any obligation to accommodate congressional needs and is not legally enforceable through a subpoena or contempt proceedings.

Members who are not committee or subcommittee chairmen sometimes seek information about executive branch programs or activities, whether for legislation, constituent service, or other legitimate purposes (such as Senators’ role in providing advice and consent for presidential appointments) in the absence of delegated oversight authority. In those non-oversight contexts, the Executive Branch has historically exercised its discretion in determining whether and how to respond, following a general policy of providing only documents and information that are already public or would be available to the public through the Freedom of Information Act, 5 U.S.C. § 552. Whether it is appropriate to respond to re-

quests from individual members will depend on the circumstances. In general, agencies have provided information only when doing so would not be overly burdensome and would not interfere with their ability to respond in a timely manner to duly authorized oversight requests. In many instances, such discretionary responses furnish the agency with an opportunity to correct misperceptions or inaccurate factual statements that are the basis for a request.

CURTIS E. GANNON
Acting Assistant Attorney General
Office of Legal Counsel



Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

June 28, 2017

Mathew M. Sturges, Staff Director

Katherine W. Dedrick, Democratic Staff Director

Tim Horne
Acting Administrator
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Mr. Horne:

I cordially invite you to present testimony at a hearing before the Subcommittee on Economic Development, Public Buildings, and Emergency Management, titled "Implementing the Federal Assets Sale and Transfer Act (FASTA): Maximizing Taxpayer Returns and Reducing Waste in Real Estate." The hearing will take place on Wednesday, July 12, 2017 at 10:00 a.m. in 2167 Rayburn House Office Building.

Please submit 100 copies of your testimony to Jack Meehan in 2165 Rayburn House Office Building by 5:00 p.m. on Monday, July 10, 2017. Please send an electronic version of your testimony to Tyler Menzler at Tyler.Menzler@mail.house.gov. Also, please be advised that oral statements to the Subcommittee will be limited to five minutes.

In compliance with the Americans with Disabilities Act, if you need any reasonable accommodations for a disability to facilitate your appearance, please contact Mike Legg at (202) 225-9446, at least two business days before the hearing.

If you or your staff have any questions or need further information, please contact Johanna Hardy of the Subcommittee at (202) 225-3014.

Sincerely,

Lou Barletta
Chairman
Subcommittee on Economic Development,
Public Buildings, and Emergency Management

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

June 28, 2017

Alan Thomas, Commissioner
Federal Acquisition Service
U.S. General Services Administration
1800 F Street, N.W.
Washington, D.C. 20006

Dear Commissioner Thomas:

The Subcommittees on Government Operations and Information Technology of the Committee on Oversight and Government Reform hereby request your testimony at a hearing on Wednesday, July 12, 2017, at 2:00 p.m. in room 2154 Rayburn House Office Building. The hearing is titled, "General Services Administration – Acquisition Oversight and Reform."

This hearing is part of a continuing oversight effort on federal acquisition oversight and reform. This effort began with a March 28, 2017, hearing titled, "Reviewing Challenges for Federal Information Technology Acquisition." The subcommittees expect to hear details on the role of the Federal Acquisition Service (FAS) in federal acquisition and the recent FAS reorganization. Further, the subcommittees expect to hear details on the role of the Technology Transformation Service (TTS), IT modernization activities and acquisition, and status of the Federal Risk and Authorization Management Program (FEDRAMP). Finally, we would like to hear GSA plans to encourage innovation and reform the federal acquisition process. You should be prepared to provide a five-minute opening statement and answer questions posed by Members.

Instructions for witnesses appearing before the Committee are contained in the enclosed Witness Instruction Sheet. In particular, please note the procedures for submitting written testimony at least two business days prior to the hearing. Please contact the Committee by **Wednesday, July 5, 2017**, to confirm your attendance. If you have any questions, please contact Julie Dunne or Katie Bailey of the House Oversight and Government Reform Committee staff at (202) 225-5074.

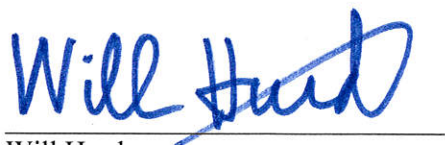


Mark Meadows
Chairman
Subcommittee on Government Operations

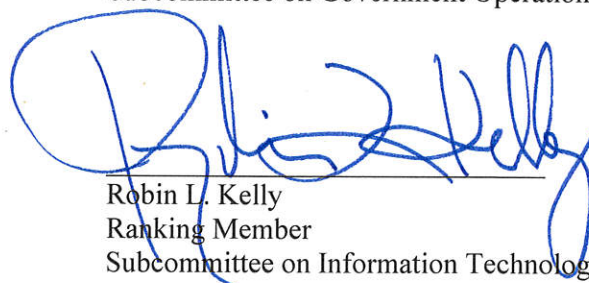
Sincerely,



Gerald E. Connolly
Ranking Member
Subcommittee on Government Operations



Will Hurd
Chairman
Subcommittee on Information Technology



Robin L. Kelly
Ranking Member
Subcommittee on Information Technology

Enclosures

Witness Instruction Sheet
Governmental Witnesses

1. Witnesses should provide their testimony via e-mail to Kiley Bidelman, Clerk, Kiley.Bidelman@mail.house.gov, no later than 10:00 a.m. two business days prior to the hearing.
2. Witnesses should also provide a short biographical summary and include it with the electronic copy of testimony provided to the Clerk.
3. At the hearing, each witness will be asked to summarize his or her written testimony in five minutes or less in order to maximize the time available for discussion and questions. Written testimony will be entered into the hearing record and may extend to any reasonable length.
4. Written testimony will be made publicly available and will be posted on the Committee's website.
5. The Committee does not provide financial reimbursement for witness travel or accommodations. Witnesses with extenuating circumstances, however, may submit a written request for such reimbursements to Robin Butler, Financial Administrator, 2157 Rayburn House Office Building, at least one week prior to the hearing. Reimbursements will not be made without prior approval.
6. Witnesses with disabilities should contact Committee staff to arrange any necessary accommodations.
7. Please note that Committee Rule 16(b) requires counsel representing an individual or entity before the Committee or any of its subcommittees, whether in connection with a request, subpoena, or testimony, promptly submit the attached notice of appearance to the Committee.
8. Committee Rules governing this hearing are online at www.oversight.house.gov.

For inquiries regarding these rules and procedures, please contact the Committee on Oversight and Government Reform at (202) 225-5074.

**COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
115TH CONGRESS**

NOTICE OF APPEARANCE OF COUNSEL

Counsel submitting: _____

Bar number: _____ **State/District of admission:** _____

Attorney for: _____

Address: _____

Telephone: (_____) _____ - _____

Pursuant to Rule 16 of the Committee Rules, notice is hereby given of the entry of the undersigned as counsel for _____ in (select one):

All matters before the Committee

The following matters (describe the scope of representation):

All further notice and copies of papers and other material relevant to this action should be directed to and served upon:

Attorney's name: _____

Attorney's email address: _____

Firm name (where applicable): _____

Complete Mailing Address: _____

I agree to notify the Committee within 1 business day of any change in representation.

Signature of Attorney

Date

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051
<http://oversight.house.gov>

June 28, 2017

Rob Cook, Deputy Commissioner & Director
Technology Transformation Services
U.S. General Services Administration
1800 F Street, N.W.
Washington, D.C. 20006

Dear Deputy Commissioner Cook:

The Subcommittees on Government Operations and Information Technology of the Committee on Oversight and Government Reform hereby request your testimony at a hearing on Wednesday, July 12, 2017, at 2:00 p.m. in room 2154 Rayburn House Office Building. The hearing is titled, "General Services Administration – Acquisition Oversight and Reform."

This hearing is part of a continuing oversight effort on federal acquisition oversight and reform. This effort began with a March 28, 2017, hearing titled, "Reviewing Challenges for Federal Information Technology Acquisition." The subcommittees expect to hear details on the role of the Federal Acquisition Service (FAS) in federal acquisition and the recent FAS reorganization. Further, the subcommittees expect to hear details on the role of the Technology Transformation Service (TTS), IT modernization activities and acquisition, and status of the Federal Risk and Authorization Management Program (FEDRAMP). Finally, we would like to hear GSA plans to encourage innovation and reform the federal acquisition process. You should be prepared to provide a five-minute opening statement and answer questions posed by Members.

Instructions for witnesses appearing before the Committee are contained in the enclosed Witness Instruction Sheet. In particular, please note the procedures for submitting written testimony at least two business days prior to the hearing. Please contact the Committee by **Wednesday, July 5, 2017**, to confirm your attendance. If you have any questions, please contact Julie Dunne or Katie Bailey of the House Oversight and Government Reform Committee staff at (202) 225-5074.



Mark Meadows
Chairman
Subcommittee on Government Operations

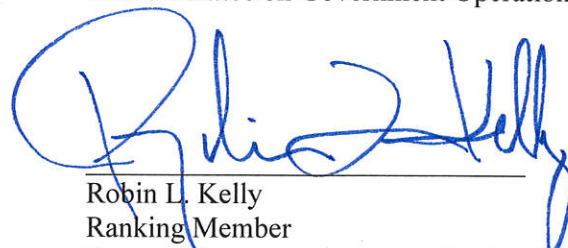
Sincerely,



Gerald E. Connolly
Ranking Member
Subcommittee on Government Operations



Will Hurd
Chairman
Subcommittee on Information Technology



Robin L. Kelly
Ranking Member
Subcommittee on Information Technology

Enclosures

Witness Instruction Sheet
Governmental Witnesses

1. Witnesses should provide their testimony via e-mail to Kiley Bidelman, Clerk, Kiley.Bidelman@mail.house.gov, no later than 10:00 a.m. two business days prior to the hearing.
2. Witnesses should also provide a short biographical summary and include it with the electronic copy of testimony provided to the Clerk.
3. At the hearing, each witness will be asked to summarize his or her written testimony in five minutes or less in order to maximize the time available for discussion and questions. Written testimony will be entered into the hearing record and may extend to any reasonable length.
4. Written testimony will be made publicly available and will be posted on the Committee's website.
5. The Committee does not provide financial reimbursement for witness travel or accommodations. Witnesses with extenuating circumstances, however, may submit a written request for such reimbursements to Robin Butler, Financial Administrator, 2157 Rayburn House Office Building, at least one week prior to the hearing. Reimbursements will not be made without prior approval.
6. Witnesses with disabilities should contact Committee staff to arrange any necessary accommodations.
7. Please note that Committee Rule 16(b) requires counsel representing an individual or entity before the Committee or any of its subcommittees, whether in connection with a request, subpoena, or testimony, promptly submit the attached notice of appearance to the Committee.
8. Committee Rules governing this hearing are online at www.oversight.house.gov.

For inquiries regarding these rules and procedures, please contact the Committee on Oversight and Government Reform at (202) 225-5074.

**COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
115TH CONGRESS**

NOTICE OF APPEARANCE OF COUNSEL

Counsel submitting: _____

Bar number: _____ **State/District of admission:** _____

Attorney for: _____

Address: _____

Telephone: (_____) _____ - _____

Pursuant to Rule 16 of the Committee Rules, notice is hereby given of the entry of the undersigned as counsel for _____ in (select one):

All matters before the Committee

The following matters (describe the scope of representation):

All further notice and copies of papers and other material relevant to this action should be directed to and served upon:

Attorney's name: _____

Attorney's email address: _____

Firm name (where applicable): _____

Complete Mailing Address: _____

I agree to notify the Committee within 1 business day of any change in representation.

Signature of Attorney

Date

Statement of Rob Cook
Deputy Commissioner and Director of Technology Transformation Services
Before the Subcommittees on Government Operations and Information
Technology of the
Committee on Oversight and Government Reform
Wednesday, July 12, 2017, at 2:00 p.m.
2154 Rayburn House Office Building
Hearing Title:
U.S. General Services Administration-Acquisition Oversight and Reform

Introduction

Good afternoon, Chairmen Meadows and Hurd, ranking members Connolly and Kelly, and members of the committees. Thank you for the opportunity to come before you to discuss the U.S. General Services Administration's Technology Transformation Services or TTS, a component of the Federal Acquisition Service. I am honored to be here sitting next to Alan Thomas, the new Commissioner of FAS.

Background

Members of this Committee are very familiar with the problems that plague Federal IT. This fiscal year, the Federal Government will spend almost \$85 billion dollars on IT projects. However, too much of this money is spent on maintaining legacy systems and networks. Even more is spent on projects that are over budget or behind schedule.

There are many root causes to these problems. Too many systems have been designed for stakeholders instead of users. Funding streams are not well aligned to the IT refresh cycle and generally don't provide enough flexibility. Furthermore, we see minimal adoption of agile development practices across the Federal landscape and a significant reluctance to implement modular procurement practices.

However, the path to a successful IT future is possible and within our grasp. Such a transformation, though, will require changes to both culture and policy. It will require hard work and sustained attention from many people, including high-level executives, program managers, and also Congress.

By improving how we buy and employ IT, by shifting away from legacy systems, and by continuing the push towards transparency and open data, I am confident that we can significantly improve Federal IT and, ultimately, how agencies serve the American people.

GSA has a significant role to play in these efforts. Historically, GSA has played a central role in supporting and assisting Federal agencies. As Alan pointed out in his testimony, one of the primary ways in which GSA has served the broader Federal IT community is by helping agencies buy and build technology and related services. We help by assisting agencies in accessing and purchasing from technology companies, informing and building out agency technology services, and building new government-wide platforms and products at scale.

Technology Transformation Services

In addition to the traditional work that GSA performs through the Federal Acquisition Service, the agency has recognized that there is a need across the Federal community for services that will help agencies think differently about how they are buying and managing information technology. TTS was created to meet this need.

The mission of TTS is simple—to improve the public’s experience with the government by helping agencies build, buy, and share technology that allows them to better serve the public.

To accomplish this, TTS applies modern methodologies and technologies in helping agencies make their services more accessible, efficient, and effective. TTS also creates government-wide products that exemplify these values. We employ modern software design, product development, and outcome measurement as we build and share technology applications and platforms with Federal agencies, all with the goal of improving the public’s experience with government.

TTS is currently made up of four main offices.

18F

First, the 18F program was created to help improve how agencies interact with their customers and the American public and to also improve how agencies buy and manage information technology. Built in the spirit of America’s top tech startups, 18F consults with agencies to help them rapidly deploy technology tools to create great services for the public. 18F hires via a “tour of duty” model and brings in talented people for short stints in the Federal Government. 18F staff are hired for two-year terms, with the ability to extend for a second two-year term.

18F seeks to provide Federal agencies with user-centric customer solutions that address a client's unique challenges. For example, 18F helped Treasury implement the DATA Act, which provides data on how the Federal Government spends money through an easy-to-use, searchable web tool. To accomplish this work, 18F assisted Treasury with agile development, public engagement, procurement strategy, and training. Treasury credits 18F's approach as a key success factor in the implementation of the DATA Act. 18F also created the U.S. Web Design Standards to guarantee readability and accessibility of government websites while saving duplicative design and development costs. The Web Design Standards are currently used by hundreds of government websites registering millions of page views every month. In addition, 18F develops high-demand products and platforms to scale and institutionalize across government. For example, 18F is currently offering a cloud platform, through a pilot program, to agencies that need such services.

Office of Products and Programs

TTS also operates the Office of Products and Programs (OPP), which helps deliver information and services to the public. OPP's origins began in GSA's Office of Citizen Services and Innovative Technologies (OCSIT). For decades, GSA has been a leader in connecting citizens with government information through traditional media such as publications and call centers or websites such as USA.gov or gobiernoUSA.gov. Prior to the creation of TTS, these programs were run out of OCSIT. Now OPP continues to deliver key government information to the public by working closely with Federal agencies and developing innovative products and services to the public.

For example, OPP operates data.gov, which is the Federal Government's portal for agency data sets. They also encourage agency use of challenge.gov, the official hub for technology challenge competitions that ask the public's help in improving information delivery. In addition, the Federal Risk and Authorization Management Program or FedRAMP was created in 2012 to help standardize and improve security for cloud products and services that help provide information to the public. OPP has five primary portfolio areas, which include Secure Cloud, Public Experience, Data Services, Innovation Portfolio, and Smarter IT Delivery.

Presidential Innovation Fellows

Next we have the Presidential Innovation Fellows program, or PIF program. The Presidential Innovation Fellows program brings the principles, values, and practices of the innovation economy into government. This highly competitive program pairs talented, diverse technologists and innovators with top civil servants and change

leaders to tackle some of government's biggest challenges. These teams address complex issues that involve people, processes, products, and policy to identify and implement solutions that achieve lasting impact.

Presidential Innovation Fellows serve for 12 months, during which they work on one or several initiatives. Fellows operate with wide latitude to allow for individual initiative in working with agencies to tackle difficult problems. They also spend a portion of their time co-working and collaborating with other Fellows. Throughout the program, Fellows receive support from partners and change agents in the White House and across various Federal agencies.

Office of Acquisitions

Finally, the Office of Acquisitions exists to help make government a better buyer of technology. The Office seeks to improve the acquisition process for TTS product leads, agency customers, and industry partners. They ensure that informed buyers are confident they are purchasing the right products and services to meet their need, and they make the acquisition process easier and more accessible. The Office seeks to design and promote acquisition approaches that are aligned with current technology-industry development practices to ensure government technology purchases have a high degree of success and meet the needs of agencies and the people they serve.

The Acquisition Office's projects include partnering with GSA's Federal Acquisition Service to create the Agile Blanket Purchase Agreement (BPA), in which vendors qualify for Schedule 70 by submitting actual code, or proof of expertise, rather than large amounts of documentation. The Agile BPA helps to attract vendors who excel in user-centered design and agile software development. In addition, the Acquisition Office helped HHS and California achieve significant savings by redesigning the procurement of California's new federally funded Child Welfare System. TTS's continued engagement led to California launching its own agile vendor pool. Through these and other efforts, the Office of Acquisition is helping agencies implement modular procurement practices and be better buyers of technology.

Conclusion: What the Future Holds

The rapid transformation of information technology and how Americans interact with private-sector companies and financial institutions has radically changed the online experience for the public.

The sea change in the digital marketplace has left Americans expecting more from their government. Meanwhile government agencies are experiencing outdated technology and lengthy IT projects that don't deliver as intended. This results in frustrating and lengthy paperwork exercises to engage with Federal agencies that are not acceptable to the general public.

Federal agencies must continue to adapt to the modern, digital world in ways that are easy and secure for the American people. We are at a crossroads—opportunities abound to better use technology to help agencies perform their missions and serve the public, and so do challenges and outside threats. The next decade will bring increasingly complex challenges, and TTS, with our ability to implement cross-government solutions, is uniquely positioned to help agencies address them.

The Committee's Modernizing Government Technology Act is a positive step to help agencies make this transition and overcome funding challenges. Providing agencies with more flexibility through individual working capital funds and a centralized Technology Modernization Fund (TMF) will help them better align agency funding to the IT refresh cycle. In particular, the centralized nature of the TMF will strengthen the ability of the Federal Government to strategically prioritize investments across government as well as inside agencies.

I speak for everyone in TTS when I tell you that we are excited to help agencies make this transition and to work with this Committee to make that happen.

Thank you for your time. I look forward to your questions.

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

July 6, 2017

Timothy O. Horne
Acting Administrator
General Services Administration
1800 F Street, NW
Washington, D.C. 20405

Dear Acting Administrator Horne:

We are writing for the third time with our request that the General Services Administration (GSA) produce documents we have requested pursuant to the statutory “Seven Member Rule.”¹

On February 8, 2017, we sent a letter requesting complete, unredacted copies of documents related to the administration of the Old Post Office lease agreement with President Donald Trump’s company, and we invoked our authority under the Seven Member Rule to make this request.²

We wrote to you after receiving a letter from GSA on February 6, 2017, stating that while the agency would not provide the documents in response to a request from a Member who is not a Committee Chairman, the agency would consider a request submitted pursuant to the Seven Member Rule.³

¹ 5 U.S.C. § 2954 (incorporating and amending 45 Stat. 996 (1928)). The statutory language refers to the “Committee on Government Operations.” The Committee was renamed several times since then, and in the 110th Congress, it was renamed the Committee on Oversight and Government Reform. References in statute to the “Committee on Government Operations” are treated as referring to the Committee on Oversight and Government Reform.

² Letter from Ranking Member Elijah E. Cummings, et al., House Committee on Oversight and Government Reform, to Acting Associate Administrator Saul Japson, General Services Administration (Feb. 8, 2017) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2017-02-08.EEC%20et%20al%20to%20Japson-GSA%20re%20Trump%20International%20Hotel.pdf>).

³ Letter from Acting Associate Administrator Saul Japson, General Services Administration, to Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform (Feb. 6, 2017) (<https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/GSA%20letter.pdf>).

In fact, your predecessor complied with a previous request we made for documents in 2016 regarding exactly the same topic, explicitly noting the agency's compliance with the Seven Member Rule.⁴

Our February 8 letter requested a response by February 13, 2017, but GSA provided no response. Committee staff emailed GSA staff on February 14, 16, 17, and 22, but never received a substantive reply. GSA staff responded to two of those emails by saying they would check on the status of the response but then stopped responding altogether.

During a briefing by GSA officials to Republican and Democratic Committee staff on April 4, 2017, our staff asked about the status of GSA's response to our request, and the GSA officials responded that they would provide a status update. Unfortunately, that never happened.

On June 5, 2017, all 18 Democratic Members of the Committee sent another letter requesting unredacted documents relating to the administration of the lease agreement pursuant to the Seven Member Rule. That letter requested:

1. all monthly reports submitted to GSA since November 2016 by Trump Old Post Office LLC describing revenues and expenses;
2. all correspondence and documents from Trump Old Post Office LLC relating to liens or any action to resolve liens;
3. all correspondence with representatives of Trump Old Post Office LLC, the Trump transition team, or the Trump Administration regarding compliance with the lease before or after the presidential election, Section 37.19 of the lease, the monthly financial reports, the structure of the trust created to address Section 37.19 of the lease, or any other matters above;
4. all correspondence and documents relating to funds received from any foreign country, foreign entity, or foreign source;
5. correspondence from Adam L. Rosen on December 16, 2016, and December 29, 2016, to GSA, referenced in the attachment to GSA's February 6, 2017, letter to Members of this Committee;
6. all correspondence and documents relating to representatives of the tenant in its interactions with GSA;
7. all documents containing legal interpretations of Section 37.19 of the lease

⁴ Letter from Lisa A. Austin, Associate Administrator, General Services Administration, to Ranking Member Elijah E. Cummings, House Committee on Oversight and Government Reform (Jan. 3, 2017) (<https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/GSA%20Response%20to%20Seven%20Member%20Rule%2001-03-17.pdf>).

created within GSA or received from the tenant;

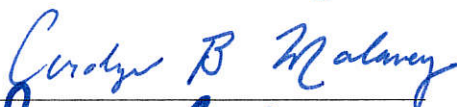
8. any legal opinion relied upon by GSA in making a determination regarding the President's compliance with Section 37.19; and
9. all drafts and edits of Kevin Terry's letter on March 23, 2017, including who authored the drafts or edits.⁵

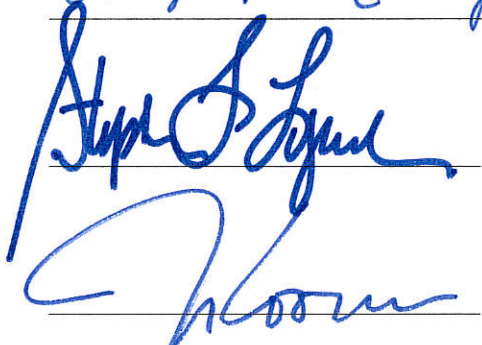
We requested that GSA provide these documents by June 23, 2017, but again, we have received no response. Committee staff emailed GSA staff on June 27, and 30, but received no reply.

If we do not receive a written response by July 20, 2017, we will have no option but to conclude that GSA has made the decision not to respond to our inquiry, and we will consider other options to enforce the Seven Member Rule.

Sincerely,


Elijah E. Cummings

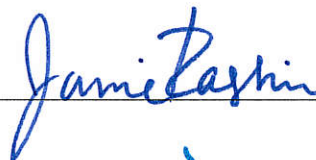

Carolyn B. Maloney


Stephen L. Solarz


Ben Ray Lujan

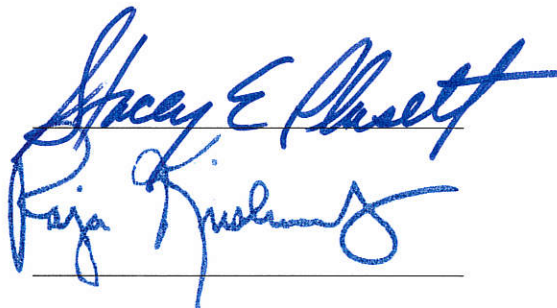

Brenda L. Lawrence

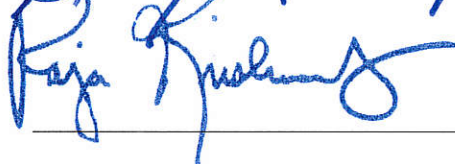

Matthew A. Cartwright


Jamie Raskin


Vee B. Dromm


Mark D. D. D.


Space E. Phaselt


Raja K. K.

⁵ Letter from Ranking Member Elijah E. Cummings, et al., House Committee on Oversight and Government Reform, to Timothy O. Horne, Acting Administrator, General Services Administration (June 5, 2017) (online at <https://democrats-oversight.house.gov/sites/democrats.oversight.house.gov/files/documents/2017-06-05.Dem%20Members%20to%20GSA%20re.Seven%20Members.pdf>).

Peter W. 04
John P. Linder

Wm. Lang Clay

cc: The Honorable Trey Gowdy, Chairman

Eleanor H. Norton

Pat. Kelly

Frank R. Dooly



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
House of Representatives
Washington, DC 20515

Dear Representative Cummings:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Carolyn Maloney
House of Representatives
Washington, DC 20515

Dear Representative Maloney:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Stephen Lynch
House of Representatives
Washington, DC 20515

Dear Representative Lynch:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Jim Cooper
House of Representatives
Washington, DC 20515

Dear Representative Cooper:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Bonnie Watson Coleman
House of Representatives
Washington, DC 20515

Dear Representative Coleman:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Brenda Lawrence
House of Representatives
Washington, DC 20515

Dear Representative Lawrence:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Matthew Cartwright
House of Representatives
Washington, DC 20515

Dear Representative Cartwright:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Jamie Raskin
House of Representatives
Washington, DC 20515

Dear Representative Raskin:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Val Butler Demmings
House of Representatives
Washington, DC 20515

Dear Representative Demmings:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Mark Desaulnier
House of Representatives
Washington, DC 20515

Dear Representative Desaulnier:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Stacey E. Plaskett
House of Representatives
Washington, DC 20515

Dear Representative Plaskett:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Raja Krishnamoorthi
House of Representatives
Washington, DC 20515

Dear Representative Krishnamoorthi:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Peter Welch
House of Representatives
Washington, DC 20515

Dear Representative Welch:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable John P. Sarbanes
House of Representatives
Washington, DC 20515

Dear Representative Sarbanes:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable William Lacy Clay
House of Representatives
Washington, DC 20515

Dear Representative Clay:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



July 17, 2017

The Honorable Eleanor Holmes Norton
House of Representatives
Washington, DC 20515

Dear Representative Norton:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Robin Kelly
House of Representatives
Washington, DC 20515

Dear Representative Kelly:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure



Office of Congressional and Intergovernmental Affairs

July 17, 2017

The Honorable Gerald E. Connolly
House of Representatives
Washington, DC 20515

Dear Representative Connolly:

The Acting Administrator requested that I respond to the letter dated July 6, 2017, signed by you and other members of the House Committee on Oversight and Government Reform (the "Committee"), requesting certain records from the U.S. General Services Administration ("GSA") related to the Old Post Office lease agreement, pursuant to 5 U.S.C. § 2954.

With regard to your inquiry about GSA's responsiveness to congressional inquiries and requests, GSA intends to respond to all congressional inquiries. However, for oversight requests, please see the enclosed Letter Opinion for the Counsel to the President. In this Letter, the U.S. Department of Justice's Office of Legal Counsel determined that:

...the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of Executive Branch programs and activities—may be exercised only by each chamber of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee.

The Letter also states:

Accordingly, the Executive Branch's longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

An identical letter has been sent to your colleagues. If you have any additional questions or concerns, please contact me at (202) 501-0563.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Brennan Hart III".

P. Brennan Hart III
Associate Administrator

Enclosure

Authority of Individual Members of Congress to Conduct Oversight of the Executive Branch

The constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of executive branch programs and activities—may be exercised only by each house of Congress or, under existing delegations, by committees and subcommittees (or their chairmen).

Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee. They may request information from the Executive Branch, which may respond at its discretion, but such requests do not trigger any obligation to accommodate congressional needs and are not legally enforceable through a subpoena or contempt proceedings.

May 1, 2017

LETTER OPINION FOR THE COUNSEL TO THE PRESIDENT

We understand that questions have been raised about the authority of individual members of Congress to conduct oversight of the Executive Branch. As briefly explained below, the constitutional authority to conduct oversight—that is, the authority to make official inquiries into and to conduct investigations of executive branch programs and activities—may be exercised only by each house of Congress or, under existing delegations, by committees and subcommittees (or their chairmen). Individual members of Congress, including ranking minority members, do not have the authority to conduct oversight in the absence of a specific delegation by a full house, committee, or subcommittee. Accordingly, the Executive Branch’s longstanding policy has been to engage in the established process for accommodating congressional requests for information only when those requests come from a committee, subcommittee, or chairman authorized to conduct oversight.

The Constitution vests “[a]ll legislative Powers” in “a Congress of the United States, which shall consist of a Senate and House of Representatives.” U.S. Const. art. I, § 1. The Supreme Court has recognized that one of those legislative powers is the implicit authority of each house of Congress to gather information in aid of its legislative function. *See McGrain v. Daugherty*, 273 U.S. 135, 174 (1927). Each house may exercise its authority directly—for example, by passing a resolution of inquiry seeking information from the Executive Branch. *See 4 Deschler’s Precedents of the United States House of Representatives*, ch. 15, § 2, at 30–50

(1981) (describing the practice of resolutions of inquiry and providing examples); Floyd M. Riddick & Alan S. Frumin, *Riddick's Senate Procedure*, S. Doc. No. 101-28, at 882 (1992) (“The Senate itself could investigate or hear witnesses as it has on rare occasions[.]”).

In modern practice, however, each house typically conducts oversight “through delegations of authority to its committees, which act either through requests by the committee chairman, speaking on behalf of the committee, or through some other action by the committee itself.” *Application of Privacy Act Congressional-Disclosure Exception to Disclosures to Ranking Minority Members*, 25 Op. O.L.C. 289, 289 (2001) (“*Application of Privacy Act*”); see also Alissa M. Dolan et al., Cong. Research Serv., RL30240, *Congressional Oversight Manual* 65 (Dec. 19, 2014). As the Supreme Court has explained, “[t]he theory of a committee inquiry is that the committee members are serving as the representatives of the parent assembly in collecting information for a legislative purpose” and, in such circumstances, “committees and subcommittees, sometimes one Congressman, are endowed with the full power of the Congress to compel testimony.” *Watkins v. United States*, 354 U.S. 178, 200–01 (1957).

By contrast, individual members, including ranking minority members, “generally do not act on behalf of congressional committees.” *Application of Privacy Act*, 25 Op. O.L.C. at 289; see also *id.* at 289–90 (concluding that “the Privacy Act’s congressional-disclosure exception does not generally apply to disclosures to ranking minority members,” because ranking minority members “are not authorized to make committee requests, act as the official recipient of information for a committee, or otherwise act on behalf of a committee”). Under existing congressional rules, those members have not been “endowed with the full power of the Congress” (*Watkins*, 354 U.S. at 201) to conduct oversight. See *Congressional Oversight Manual* at 65; see also *Exxon Corp. v. FTC*, 589 F.2d 582, 593 (D.C. Cir. 1978) (“[D]isclosure of information can only be compelled by authority of Congress, its committees or subcommittees, not solely by individual members; and only for investigations and congressional activities.”). Individual members who have not been authorized to conduct oversight are entitled to no more than “the *voluntary* cooperation of agency officials or private persons.” *Congressional Oversight Manual* at 65 (emphasis added).

The foregoing reflects the fundamental distinction between constitutionally authorized oversight and other congressional requests for infor-

mation. When a committee, subcommittee, or chairman exercising delegated oversight authority asks for information from the Executive Branch, that request triggers the “implicit constitutional mandate to seek optimal accommodation . . . of the needs of the conflicting branches.” *United States v. AT&T Co.*, 567 F.2d 121, 127 (D.C. Cir. 1977); *see also id.* at 130–131 (describing the “[n]egotiation between the two branches” as “a dynamic process affirmatively furthering the constitutional scheme”). Such oversight requests are enforceable by the issuance of a subpoena and the potential for contempt-of-Congress proceedings. *See McGrain*, 273 U.S. at 174; 2 U.S.C. §§ 192, 194; *see also* Standing Rules of the Senate, Rule XXVI(1), S. Doc. No. 113-18, at 31 (2013) (empowering all standing committees to issue subpoenas); Rules of the House of Representatives, 115th Cong., Rule XI, cl. 2(m)(1) (2017) (same). Upon receipt of a properly authorized oversight request, the Executive Branch’s longstanding policy has been to engage in the accommodation process by supplying the requested information “to the fullest extent consistent with the constitutional and statutory obligations of the Executive Branch.” Memorandum for the Heads of Executive Departments and Agencies from President Ronald Reagan, *Re: Procedures Governing Responses to Congressional Requests for Information* (Nov. 4, 1982). But a letter or inquiry from a member or members of Congress not authorized to conduct oversight is not properly considered an “oversight” request. *See Congressional Oversight Manual* at 56 (“Individual Members, Members not on a committee of jurisdiction, or minority Members of a jurisdictional committee, may, like any person, request agency records. When they do, however, they are not acting pursuant to Congress’s constitutional authority to conduct oversight and investigations.”). It does not trigger any obligation to accommodate congressional needs and is not legally enforceable through a subpoena or contempt proceedings.

Members who are not committee or subcommittee chairmen sometimes seek information about executive branch programs or activities, whether for legislation, constituent service, or other legitimate purposes (such as Senators’ role in providing advice and consent for presidential appointments) in the absence of delegated oversight authority. In those non-oversight contexts, the Executive Branch has historically exercised its discretion in determining whether and how to respond, following a general policy of providing only documents and information that are already public or would be available to the public through the Freedom of Information Act, 5 U.S.C. § 552. Whether it is appropriate to respond to re-

Opinions of the Office of Legal Counsel in Volume 41

quests from individual members will depend on the circumstances. In general, agencies have provided information only when doing so would not be overly burdensome and would not interfere with their ability to respond in a timely manner to duly authorized oversight requests. In many instances, such discretionary responses furnish the agency with an opportunity to correct misperceptions or inaccurate factual statements that are the basis for a request.

CURTIS E. GANNON
Acting Assistant Attorney General
Office of Legal Counsel

**“Implementing the Federal Assets Sale and Transfer Act (FASTA):
Maximizing Taxpayer Returns and Reducing Waste in Real Estate”
Subcommittee on Economic Development, Public Buildings, and
Emergency Management Hearing
Wednesday, July 12, 2017, 10:00 a.m.
2167 Rayburn House Office Building
Washington, D.C.**

Questions for the Record

Submitted on behalf of Representative Lou Barletta (R-PA)

1. GSA and the Department of Veterans Affairs (VA) have been working closely with the City of Pittsburgh, PA, in the disposing of the vacant VA Highland Drive Medical Facility. The traditional real property disposal process can be cumbersome. However, there are ways the process could be streamlined and move faster – such as completing certain reviews simultaneously.

a. What is GSA doing to look for opportunities to streamline the process?

Prior to the U.S. General Services Administration’s (GSA) formal involvement in the Pittsburgh property, VA sought assistance from GSA. On May 11, 2016, months before the facility was reported excess, GSA conducted a Targeted Asset Review (TAR). This analysis provided VA with important due diligence information that VA used to submit the necessary documents to submit the finalized Report of Excess and officially begin the disposal process. Concurrent with the completion of the TAR and submission of the Report of Excess, GSA began meeting with Pittsburgh city officials to gain an understanding of the city’s plans for the property. As GSA and VA continued to interact with local stakeholders, and identified that VA needed to complete the Environmental Phase I site assessment and the boundary and utility survey. As GSA waited for the development of these documents, GSA and VA proceeded with the disposal process and would complete the required reports together as the disposal process moved forward. Concurrent to the development of the documents, GSA initiated the Federal Screening process. On July 20, 2017, GSA completed Federal Screening, the first step in the Title 40 disposal process. GSA can report that the property is now surplus to the needs of the Federal Government, and the agency continues to work with the city to better understand its proposed uses. By advancing the disposal process while also confirming the environmental conditions of the reported property, GSA estimates that 3 months were saved on the disposition of the asset.

These efforts have been made simultaneously, with an eye to the most efficient and comprehensive repositioning of the 167-acre facility.

- b. Do you commit to providing regular updates to the Committee as the disposal progresses?

Yes. To date, GSA has provided several status updates and has committed to continue with monthly briefings for Committee staff and other congressional stakeholders.

- c. What is your current timetable for the disposal?

GSA estimates that the transfer of ownership of the property will be completed by April 2018. This timeframe depends on the disposal methods and on environmental issue and/or title conditions.

2. The Federal Assets and Sale Transfer Act (FASTA) establishes requirements for the Federal Real Property Profile database and requires that the database be publicly accessible.

- a. Where is GSA in implementing these requirements?

GSA has collected data from agencies as required by FASTA. GSA is reviewing the data collected and working with agencies to identify data elements that should be excluded for reasons of national security (as defined by the Department of Homeland Security Interagency Security Committee) and the Freedom of Information Act. Once final determinations are made, the data will be made available to the public.

- b. Will the deadline of one year from enactment be met?

GSA is continuing to work closely with OMB, DHS, and all Federal agencies reporting data to the FRPP database to prepare the data for publication. GSA is on course to make the data accessible by the December 16, 2017, deadline.

3. In 2014, the Subcommittee launched a series of hearings and roundtables focused on the large number of leases that will be expiring in the near term and how we can ensure GSA is in the best position to negotiate good deals and lower rates for the taxpayer when replacing those leases. At that time, we found 50 percent of GSA's leases were expiring in five years. We also found a potential for significant savings of more than 20 percent if GSA negotiated longer term deals, as opposed to firm terms of

five years or short-term extensions. Given the potential savings and large number of expiring leases, last Congress, I introduced bipartisan legislation, the Public Buildings Reform and Savings Act of 2016, which passed the House. That legislation would have created a streamlined leasing pilot program to provide GSA more tools to replace expiring leases with good deals. While I plan to re-introduce similar legislation, there are steps GSA can take now to lower leasing costs such as eliminating holdovers, negotiating replacement leases with firm terms exceeding five years, and working across tenant agencies to find opportunities to co-locate and consolidate as leases expire.

a. What steps has GSA taken to position itself to negotiate better lease deals?

GSA agrees with your assessment of the opportunities to save significant tax dollars through the replacement of GSA's expiring leases. In addition, GSA believes the likelihood of realizing these savings greatly improves when there is alignment between the executive and legislative branches on the goal and strategies for achieving these savings. To that end, GSA looks forward to partnering with the committee in this effort. Specifically, GSA is pursuing two powerful strategies for reducing lease costs. These are reducing the square footage of replacement leases when it is cost effective and increasing the firm term of midsize and large leases. These strategies have the potential to generate significant savings over the life of the leases, and GSA will use them aggressively when they result in taxpayer savings.

Additionally, GSA is leveraging OMB's Reduce the Footprint (RTF) policy to identify leases for consolidation and disposal, as well as using the agency specific office space design standard requirement per the RTF policy to encourage agencies to downsize and efficiently design new office acquisitions.

Furthermore, in our efforts to improve the delivery of leased space, in 2015, GSA rolled out its online leasing platform, known as the "Automated Advanced Acquisition Program" (AAP), in all markets in the United States. The goals for the platform are to make it easier for the real estate industry to do business with the Federal Government, for GSA to deliver leased space more quickly to its Federal customer agencies, and for GSA to receive competitive lease rates. AAP's paperless online offer submission process enables the Government to accomplish these goals.

GSA also utilizes the GSA Leasing Support Services (GLS) contract. GLS provides support services via a vendor broker to the GSA lease contracting officers and leasing specialists during the procurement process (e.g., market surveys, site visits, document preparation, and negotiations). GLS serves as a resource multiplier for the regional GSA leasing offices. The contract enables

GSA to leverage broker expertise, market knowledge, and existing industry commission practices for compensating brokers.

GSA is implementing a long-term lease strategy in which GSA considers the benefits of favorable rental pricing associated with longer firm terms against the costs associated with the risk of the inability to backfill vacant Government-controlled space. Specifically, GSA is striving to:

- Obtain lower rental rates by better leveraging GSA's financial strength and its 20-year lease acquisition authority through longer leases where appropriate;
- Reduce the number of lease procurements and the resulting workload burden on regions by using strategies for longer lease terms; and
- Implement these strategies in a manner that does not result in a material increase in vacant leased space.

Overall, the firm term of all new lease solicitations should more closely match the expected need for the space by the Government, and not necessarily match the length of a particular agency's use of that space.

GSA has been working with its customer agencies to emphasize the importance of earlier planning for upcoming lease expirations. The earlier development of customer agency requirements allows not only for footprint reduction, but also allows GSA to make progress in reducing costly extensions, securing longer term leases, and ensuring a competitive approach in its procurements. In FY 2017, the agency continued to sign a growing number of long-term leases (26 percent compared to 20 percent in FY 2015). Also, since FY 2015, GSA reduced the amount of vacant leased space from 1,350,502 square feet to 848,382 square feet.

- b. Please provide the Committee the percentage and square footage of expiring leases over the next five years.

Between FY 2017 and FY 2022, 62 percent of leases and 56 percent of leased rentable square feet, amounting to 106 million rentable square feet, will expire.

- c. Please provide the Committee the number and percentage of leases in holdovers and in short-term extensions.

As of September 2017, 74 leases (.09 percent of the leased inventory) with private entities are in holdover status, and 113 leases (1.4 percent of the leased inventory) are in short-term (less than a year) extensions.

Submitted on behalf of Representative Peter A. DeFazio (D-OR)

1. Please provide the following records in the possession of the GSA to the Committee in unredacted form:

a. All communications that took place from June 16, 2015, to the present related to the Old Post Office building lease agreement (GS-LS-11-1307) between contracting officer Kevin Terry, or any other GSA employee, and

- i. Donald J. Trump,
- ii. Ivanka Trump,
- iii. Donald Trump Jr.,
- iv. Eric Trump, or
- v. David Orowitz.

GSA is providing documents that are responsive to this question.

b. All communications between Timothy Horne and

- i. the Donald J. Trump campaign for president, or
- ii. the Donald J. Trump presidential transition.

GSA is providing documents that are responsive to this question.

c. All legal memos or opinions created pursuant to the Old Post Office lease agreement.

In accordance with the July 20, 2017, letter from Marc Short, White House Director of Legislative Affairs, to Senator Grassley, GSA will “use its best efforts to be as timely and responsive as possible in answering such requests consistent with the need to prioritize requests from congressional Committees...with any legitimate confidentiality or other interest of the Executive Branch.” Since answering the question could involve “legitimate confidentiality or other interests of the Executive Branch,” GSA respectfully declines to provide an answer.

d. All formal notices pursuant to the Old Post Office lease agreement

- i. from GSA to the tenant
- ii. from the tenant to GSA

GSA is providing documents that are responsive to this question.

- e. All monthly reports submitted by the tenant describing revenues, expenses, and budgets, pursuant to the Old Post Office lease agreement.

GSA is providing documents that are responsive to this question.

- f. All guidance provided by the White House or any other federal agency related to the Old Post Office lease agreement.

GSA has not received any guidance from the White House or any other Federal agency related to this lease agreement.

- 2. Please provide an explanation of how profits generated by the Trump International Hotel are calculated, and the amounts that GSA is entitled to receive on an annual or monthly basis. Specifically, please describe:

- a. How often Trump International Hotel calculates the profits,

GSA is unaware of how often the Trump Old Post Office LLC calculates any such profits. The lease requires the LLC to pay a minimum annual base rent of \$3 million, escalated on an annual basis at the consumer price index. The LLC also will pay a percentage rent difference if the percentage of gross revenues exceeds the minimum base rent payment.

- b. How often profit information is provided to GSA,

The lease establishes a number of different reporting requirements. In particular, Section 5.3(b) of the lease requires the submission of an annual audited financial statement, which sets forth, among other things, gross operating profit.

- c. Eligible expenses that are itemized by Trump International Hotel,

The lease establishes a number of different reporting requirements. In particular, Section 5.3(b) requires the submission of an annual audited financial statement, and Section 5.3(c) requires the submission of a monthly statement. However, nothing in the lease requires an itemization of "eligible expenses."

- d. Projected revenue information provided by Trump International Hotel, and

Because the terms and conditions of the lease do not require the tenant to provide this information, GSA is not able to respond to this question.

- e. Any mechanisms GSA is entitled to use to validate profit calculations.

Section 5.4 of the lease provides GSA with audit rights.

- 3. Please provide profit statements for the Trump International Hotel for 2016, and for January through June 2017.

GSA does not receive a separate document entitled "profit statements," The hotel officially opened for business on October 26, 2016. The first annual statement for the initial year of the hotel being open for business is not due until the end of December 2017.

- 4. Please provide any guidance provided by the White House or any other federal agency to GSA with regard to the Old Post Office lease agreement.

GSA did not receive any guidance from the White House or any other Federal agency with regard to the Old Post Office lease agreement.

- 5. Are any of the following White House employees recused from participating in decisions related to the Old Post Office lease? Please provide documentation; if none, please explain.

- a. Ivanka Trump
- b. Jared Kushner

GSA is not aware of whether these individuals have been recused from participating in decisions related to the Old Post Office lease. GSA is not in possession of any documentation regarding this question. Neither person is a GSA employee.

Submitted on behalf of Representative Jeff Denham (R-CA)

- 1. How many agencies met the April 15, 2017 date for providing data on owned, leased, or controlled properties to GSA?

In response to GSA's request, over 50 agencies provided data on owned, leased, or otherwise controlled real property by April 15, 2017.

GSA also requested information from all Chief Financial Officer Act agencies for recommendations to the Real Property Reform Board.

1. Did those agencies include recommendations of unneeded properties?

Yes, agencies submitted recommendations as required by the act.

2. How do you recommend we incentivize more agencies to participate and submit that data and their valuable properties for consideration?

Full funding of the President's FY 2018 request for the Board salaries and expenses as well as the Asset Proceeds and Space Management Fund to support project implementation would incentivize greater participation.

2. Upon receipt of agency recommendations, the Public Buildings Reform Board is to identify and implement an accounting system to evaluate costs and returns. Additionally, GSA and Office of Management and Budget (OMB) are to develop standards and criteria against which the recommendations will be reviewed. Has GSA begun consultation with OMB to review recommendations and develop standards for review?

Yes, recommendations have been reviewed and standards have been developed in consultation with OMB.

3. On July 11, 2017, GSA announced that it is cancelling the strategy for the new FBI headquarters proposal. Trading the value of the Hoover building towards the value of the new property and offsetting the delta with appropriations was a questionable strategy. But we now have an opportunity: the FBI project is perfectly situated to be sold under FASTA authority. Does GSA plan to move forward with finding a new FBI headquarters or just cancel the project?

1. Does GSA plan to explore FASTA authority for the project?

GSA and the FBI are currently working to identify acquisition solutions to meet the requirements of the new FBI headquarters. GSA and the FBI are working to report back to Congress by November 30, 2017.

2. Which type of transactions does GSA plan to explore for the project?

GSA and the FBI are currently working to identify acquisition solutions to meet the requirements of the new FBI headquarters. GSA and the FBI are working to report back to Congress by November 30, 2017.

Submitted on behalf of Representative Barbara Comstock (R-VA)

Questions regarding the Federal Real Property Profile (FRPP):

1. By way of background, the House Appropriations Committee included the following language in its Committee Report to Accompany the Financial Services and General Government Appropriations Act for Fiscal Year 2018:

Federal Real Property Profile.—The Committee remains extremely frustrated with the slow pace at which GSA and other federal agencies are improving the accuracy of the Federal Real Property Profile. The U.S. Government Accountability Office (GAO) named managing federal real property to its 2017 High Risk List. The Committee is concerned that despite language in the fiscal year 2015, 2016, and 2017 reports, GSA has not made progress on the value and accuracy of its inventory, taken steps to include public lands as required by Executive Order 13327, made the FRPP available to the public, or geo-enabling the FRPP. The Committee is outraged that the federal government cannot provide an accurate accounting to the American public of all the property that it owns. The Committee expects GSA to work with agencies across government and utilize geographic information technology to improve the data contained in this report and enhance transparency to the American taxpayer. The Committee directs GSA to report to the Committees on Appropriations of the House and Senate on steps taken to improve the quality and transparency of the profile within 60 days after the enactment of this Act.

For reference, the language can be viewed here

<https://appropriations.house.gov/uploadedfiles/fsgg.report.07.13.17.pdf>.

- a. What is the status of GSA's undertaking for improving and enhancing the FRPP?

GSA continues to take steps to improve the quality of data agencies submit to the FRPP. A complete status is covered in GSA's response dated August 21, 2017, to the Committee Report issued by House Appropriations Committee for the Financial Services and General Government Appropriations Act for Fiscal Year 2018.

GSA has included a copy of that report on the enclosed thumb drive.

- b. Since the GAO again included this topic in the 2017 High Risk List, will you share with me at the end of the 60-day period what steps GSA has taken to improve the FRPP?

GSA continues to take steps to improve the quality of data agencies submit to the FRPP. A complete status is covered in GSA's response dated August 21, 2017, to the Committee Report issued by House Appropriations Committee for the Financial Services and General Government Appropriations Act for Fiscal Year 2018.

GSA has included a copy of that report on the enclosed thumb drive.

2. Last year, then-GSA Administrator Denise Turner Roth stated that GSA hopes to work with the private sector as much as possible.

- a. With respect to the GSA FRPP, what has GSA done to bring out the best mapping and geospatial knowledge base and expertise from the private sector to help with the FRPP?

GSA has engaged in discussions with private sector entities as well as Federal personnel about geospatially displaying FRPP data. GSA has developed the Real Property Management Tool and the Asset Consolidation Tool—geospatial tools for federal agencies submitting data to the FRPP that allow these agencies to visually display their data to identify potential opportunities for consolidations and co-locations.

GSA is also working within the executive branch to determine what data should be made publicly accessible in accordance with FASTA requirements concerning national security and FOIA exemptions.

- b. What specifically does GSA plan to do with the geospatial community to make the FRPP more transparent and user-friendly for Members of Congress, decision-makers at the federal level, and most importantly, for my constituents searching for such data back in my district?

GSA will comply with the FASTA requirement to make the FRPP data publicly accessible, with the exception of data concerning national security and FOIA exemptions.

Questions regarding decision to halt consolidation of new FBI headquarters building:

1. My constituents and I were very troubled to learn that GSA was halting the process to consolidate the FBI headquarters building. These brave men and women really need this project to be completed in a timely and cost-efficient manner. They are currently in more than a dozen leased locations, in addition to the headquarters building. A consolidated headquarters would address security and operational concerns as well as save taxpayer dollars. In 2011, the FBI originally proposed completing the project through a ground-lease/leaseback arrangement. Instead, the GSA proceeded with an exchange approach, asserting the value of the Hoover building would be enough to cover the cost of a new consolidated headquarters. However, subsequently, GSA and the FBI returned to Congress seeking an additional \$1.4 billion in appropriations on top of the exchange.

There are less complicated ways for this project to proceed, such as what was originally proposed by the FBI.

a. Does GSA commit to considering all of these options in finding a path forward on this critical project?

GSA is looking at all options.

b. What is GSA's timeline for proposing a path forward?

GSA and the FBI are currently working to identify acquisition solutions to meet the requirements of the new FBI headquarters. GSA and the FBI are working to report back to Congress by November 30, 2017.



**Committee on Transportation and Infrastructure
U.S. House of Representatives**

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

July 28, 2017

Mathew M. Sturges, Staff Director

Katherine W. Dedrick, Democratic Staff Director

Mr. Timothy Horne
Acting Administrator
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Mr. Horne:

Thank you for your testimony before the Subcommittee on Economic Development, Public Buildings and Emergency Management at the hearing titled "Implementing the Federal Assets Sale and Transfer Act (FASTA): Maximizing Taxpayer Returns and Reducing Waste in Real Estate" held on Wednesday, July 12, 2017. As a follow-up to that hearing, attached, please find questions submitted for the record by members of the committee for your response.

Your timely and expeditious responses to these questions are much appreciated. Please respond to these requests at your earliest convenience, but no later than Friday, August 11, 2017. Please provide an electronic version of your responses to Tyler.Menzler@mail.house.gov.

Should you have any questions, please contact the Economic Development, Public Buildings, and Emergency Management Subcommittee Counsel, Johanna Hardy, at (202) 225-3014.

Sincerely,

Lou Barletta
Chairman
Subcommittee on Economic Development,
Public Buildings, and Emergency Management

Enclosure

**“Implementing the Federal Assets Sale and Transfer Act (FASTA):
Maximizing Taxpayer Returns and Reducing Waste in Real Estate”
Subcommittee on Economic Development, Public Buildings, and
Emergency Management Hearing
Wednesday, July 12, 2017, 10:00 a.m.
2167 Rayburn House Office Building
Washington, D.C.**

Questions for the Record

Submitted on behalf of Representative Lou Barletta (R-PA)

1. GSA and the Department of Veterans Affairs (VA) have been working closely with the City of Pittsburgh, PA in the disposing of the vacant VA Highland Drive Medical Facility. The traditional real property disposal process can be cumbersome. However, there are ways the process could be streamlined and move faster – such as completing certain reviews simultaneously.
 - a. What is GSA doing to look for opportunities to streamline the process?
 - b. Do you commit to providing regular updates to the Committee as the disposal progresses?
 - c. What is your current timetable for the disposal?
2. The Federal Assets and Sale Transfer Act (FASTA) establishes requirements for the Federal Real Property Profile database and requires that the database be publicly accessible.
 - a. Where is GSA in implementing these requirements?
 - b. Will the deadline of one-year from enactment be met?
3. In 2014, the Subcommittee launched a series of hearings and roundtables focused on the large number of leases that will be expiring in the near term and how we can ensure GSA is in the best position to negotiate good deals and lower rates for the taxpayer when replacing those leases. At that time, we found 50 percent of GSA’s leases were expiring in five years. We also found a potential for significant savings of more than 20 percent if GSA negotiated longer term deals, as opposed to firm terms of five years or short-term extensions. Given the potential savings and large number of expiring leases, last Congress, I introduced bipartisan legislation, the Public Buildings Reform and Savings Act of 2016 which passed the House. That legislation would have created a streamlined leasing pilot program to provide GSA more tools to replace expiring leases with good deals. While I plan to re-introduce similar legislation, there are steps GSA can take now to lower leasing costs such as eliminating holdovers, negotiating replacement leases with

firm terms exceeding five years, and working across tenant agencies to find opportunities to co-locate and consolidate as leases expire.

- a. What steps has GSA taken to position itself to negotiate better lease deals?
- b. Please provide the Committee the percentage and square footage of expiring leases over the next five years.
- c. Please provide the Committee the number and percentage of leases in holdovers and in short-term extensions.

Submitted on behalf of Representative Peter A. DeFazio (D-OR)

1. Please provide the following records in the possession of the GSA to the Committee in unredacted form:
 - a. All communications that took place from June 16, 2015 to the present related to the Old Post Office building lease agreement (GS-LS-11-1307) between contracting officer Kevin Terry, or any other GSA employee, and
 - i. Donald J. Trump
 - ii. Ivanka Trump,
 - iii. Donald Trump Jr.,
 - iv. Eric Trump, or
 - v. David Orowitz.
 - b. All communications between Timothy Horne and
 - i. the Donald J. Trump campaign for president, or
 - ii. the Donald J. Trump presidential transition.
 - c. All legal memos or opinions created pursuant to the Old Post Office lease agreement.
 - d. All formal notices pursuant to the Old Post Office lease agreement
 - i. from GSA to the tenant
 - ii. from the tenant to GSA
 - e. All monthly reports submitted by the tenant describing revenues, expenses, and budgets, pursuant to the Old Post Office lease agreement.
 - f. All guidance provided by the White House or any other federal agency related to the Old Post Office lease agreement.
2. Please provide an explanation of how profits generated by the Trump International Hotel are calculated, and the amounts that GSA is entitled to receive on an annual or monthly basis. Specifically, please describe:
 - a. How often Trump International Hotel calculates the profits,
 - b. How often profit information is provided to GSA,
 - c. Eligible expenses that are itemized by Trump International Hotel,
 - d. Projected revenue information provided by Trump International Hotel, and
 - e. Any mechanisms GSA is entitled to use to validate profit calculations.
3. Please provide profit statements for the Trump International Hotel for 2016, and for

January through June 2017.

4. Please provide any guidance provided by the White House or any other federal agency to GSA with regard to the Old Post Office lease agreement.
5. Are any of the following White House employees recused from participating in decisions related to the Old Post Office lease? Please provide documentation; if none, please explain.
 - a. Ivanka Trump
 - b. Jared Kushner

Submitted on behalf of Representative Jeff Denham (R-CA)

1. How many agencies met the April 15, 2017 date for providing data on owned, leased, or controlled properties to GSA?
 - a. Did those agencies include recommendations of unneeded properties?
 - b. How do you recommend we incentivize more agencies to participate and submit that data and their valuable properties for consideration?
2. Upon receipt of agency recommendations, the Public Buildings Reform Board is to identify and implement an accounting system to evaluate costs and returns. Additionally, GSA and Office of Management and Budget (OMB) are to develop standards and criteria against which the recommendations will be reviewed. Has GSA begun consultation with OMB to review recommendations and develop standards for review?
3. On July 11, 2017 GSA announced that it is cancelling the strategy for the new FBI headquarters proposal. Trading the value of the Hoover building towards the value of the new property and offsetting the delta with appropriations was a questionable strategy. But we now have an opportunity: the FBI project is perfectly situated to be sold under FASTA authority. Does GSA plan to move forward with finding a new FBI headquarters or just cancel the project?
 - a. Does GSA plan to explore FASTA authority for the project?
 - b. Which type of transactions does GSA plan to explore for the project?

Submitted on behalf of Representative Barbara Comstock (R-VA)

Questions regarding the Federal Real Property Profile (FRPP):

1. By way of background, the House Appropriations Committee included the following language in its Committee Report to Accompany the Financial Services and General Government Appropriations Act for Fiscal Year 2018:

Federal Real Property Profile.—The Committee remains extremely frustrated with the slow pace at which GSA and other federal agencies are improving the accuracy of the

Federal Real Property Profile. The U.S. Government Accountability Office (GAO) named managing federal real property to its 2017 High Risk List. The Committee is concerned that despite language in the fiscal year 2015, 2016, and 2017 reports, GSA has not made progress on the value and accuracy of its inventory, taken steps to include public lands as required by Executive Order 13327, made the FRPP available to the public, or geo-enabling the FRPP. The Committee is outraged that the federal government cannot provide an accurate accounting to the American public of all the property that it owns. The Committee expects GSA to work with agencies across government and utilize geographic information technology to improve the data contained in this report and enhance transparency to the American taxpayer. The Committee directs GSA to report to the Committees on Appropriations of the House and Senate on steps taken to improve the quality and transparency of the profile within 60 days after the enactment of this Act.

For reference, the language can be viewed here

<https://appropriations.house.gov/uploadedfiles/fsagg.report.07.13.17.pdf>.

- a. What is the status of GSA's undertaking for improving and enhancing the FRPP?
 - b. Since the GAO again included this topic in the 2017 High Risk List, will you share with me at the end of the 60-day period what steps GSA has taken to improve the FRPP?
2. Last year, then-GSA Administrator Denise Turner Roth stated that GSA hopes to work with the private sector as much as possible.
 - a. With respect to the GSA FRPP, what has GSA done to bring out the best mapping and geospatial knowledge base and expertise from the private sector to help with the FRPP?
 - b. What specifically does GSA plan to do with the geospatial community to make the FRPP more transparent and user-friendly for Members of Congress, decision-makers at the federal level, and most importantly, for my constituents searching for such data back in my district?

Questions regarding decision to halt consolidation of new FBI headquarters building:

1. My constituents and I were very troubled to learn that GSA was halting the process to consolidate the FBI headquarters building. These brave men and women really need this project to be completed in a timely and cost-efficient manner. They are currently in more than a dozen leased locations, in addition to the headquarters building. A consolidated headquarters would address security and operational concerns as well as save taxpayer dollars. In 2011, the FBI originally proposed completing the project through a ground-lease/leaseback arrangement. Instead, the GSA proceeded with an exchange approach, asserting the value of the Hoover building would be enough to cover the cost of a new consolidated headquarters. However, subsequently, GSA and the FBI returned to Congress seeking an additional \$1.4 billion in appropriations on top of the exchange.

There are less complicated ways for this project to proceed, such as what was originally proposed by the FBI.

- a. Does GSA commit to considering all of these options in finding a path forward on this critical project?
- b. What is GSA's timeline for proposing a path forward?

**Committee on Transportation
and Infrastructure**

**U.S. House of Representatives
Washington, DC 20515-6256**

OFFICIAL BUSINESS



Bill Shuster

Tim Horne
Acting Administrator
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405 H



GAPVSP1 20405



Questions for The Honorable Alan Thomas
Commissioner
General Services Administration, Federal Acquisition Service

Questions for the Record from Chairman Mark Meadows Subcommittee on Government Operations
House Committee on Oversight and Government Reform

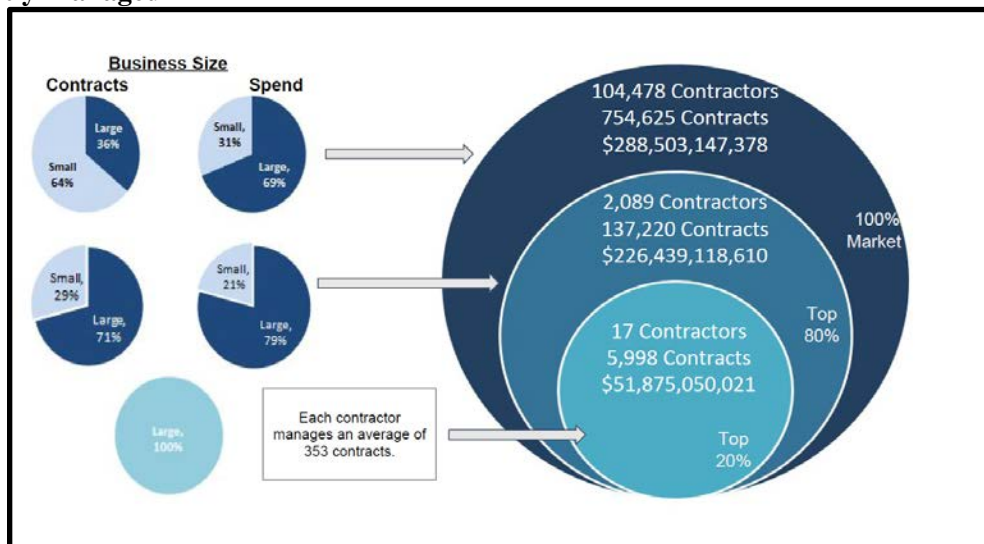
July 12, 2017, Hearing: "General Services Administration -Acquisition Oversight and Reform"

1. What do you see as GSA's best opportunity to streamline federal acquisition?

As part of the Agency Reform Plan that was recently sent to the Office of Management and Budget, GSA is exploring ways to streamline and reduce duplication in the GSA Schedules program and offer agencies expertise, improved supplier relationship management and modernized etools and purchasing platforms. Although it may ultimately require a multi-year process, streamlining and consolidating Schedules could offer significant end-to-end benefits to federal agencies, industry, and the taxpayer.

As illustrated below, there is a tremendous opportunity to significantly reduce contract duplication across government, which will result in substantial savings to agencies, industry and ultimately the American taxpayer.

FY 2016 10 Government-wide Spend Categories - Industrial Base by Spend and Contracts Currently Managed



2. How does GSA ensure the federal acquisition process reflects commercial best practices including reasonable pricing in acquisition vehicles, such as GSA schedule contracting?

The Multiple Award Schedules process for awarding a contract follows the Federal Acquisition Regulations (FAR) for “best value”. The factors considered in the process of identifying the best value for commercial products includes: warranty, delivery, price, and volume. MAS CO’s are required to stay current with their education and certification of their warrants and training includes updates and best practices as experienced across the program and made to regulation. It is the goal of FAS to provide GSA Contracting Officers and customer agencies with the latest and most accurate pricing intelligence to ensure procurements are made in the best interest of the Federal Government.

3. How many Federal Acquisition Regulation (FAR) and General Services Acquisition Regulation (GSAR) clauses apply for the acquisition of commercial goods and services? Please provide a list with title and cite for the clause.

While the actual number varies depending on requirements, up to 120 FAR and 70 GSAR clauses and provisions could apply to the acquisition of commercial items. Attached is a spreadsheet with FAR and GSAR Clauses/Provisions applicable to the acquisition of commercial items on the Multiple Award Schedule (MAS) (see attached document: FINAL MAS FAR and GSAR Clauses/Provisions Applicable to the Acq. of Commercial Items (tab 1) and FAR and GSAR- MAS clauses and provisions (tab 2)).

4. How will you use GSA's membership on the FAR Council to assess the current FAR and reduce the regulatory/compliance costs for federal contractors?

In accordance with Executive Order 13777, GSA’s regulatory reform task force is in the process of reviewing the regulations issued by GSA, including the GSA Acquisition Regulations, to identify opportunities to streamline acquisition and eliminate compliance costs for federal contractors. GSA solicited public comment through the Federal Register on May 30, 2017 for acquisition regulations reform ideas. As a member of the FAR Council, GSA will share the regulatory reform ideas with the other members of the FAR Council.

5. Currently, what services/tools does FAS provide to other agencies to assist with IT modernization and acquisition?

GSA provides a number of direct services, platforms and tools which assist Federal agencies in modernizing their IT and acquiring IT products and services.

For example, the Federal Acquisition Service (FAS) manages several large government-wide IT acquisition contracts through which agencies purchase more than \$20 billion in IT products and services each year. IT Schedule 70 features more than 4700 highly qualified vendors, including Original Equipment Manufacturers (OEMs) and Value-added Resellers (VARs). Alliant, Alliant Small Business, VETS and 8(a) STARS are IT services government-wide acquisition contracts (GWACs) providing pools of highly qualified vendors, including small businesses. Additionally, GSA recently awarded the Enterprise Infrastructure Solutions (EIS) contract to replace the expiring Networx contract, ushering in the next generation of telecommunications and related products and services and providing these services to agencies at significant savings.

Also, the Technology Transformation Services (TTS/18F), built in the spirit of tech startups, acts as a consultancy for government, enabling agencies to rapidly deploy tools and services to create services for the public. Along with inter-governmental consultant services, TTS’ Office of Products and Programs (OPP), provides platforms and products agencies can utilize to more rapidly deploy IT capabilities into their enterprise. One example is Cloud.gov, a product built and maintained by TTS that provides mature

cloud hosting services to agencies.

Additionally, GSA's Office of Governmentwide Policy (OGP) works directly with the Office of Management and Budget (OMB) on the Data Center Optimization Initiative (DCOI). The DCOI directly supports the Federal Information Technology Acquisition Reform Act (FITARA) of 2014 and provides agencies with support as they modernize and optimize their Data Centers.

These are just a few examples of the robust portfolio of IT services that GSA can bring to bear to assist agencies in modernizing their IT portfolio.

6. On July 6, 2017, GSA settled a whistleblower case brought by former Commissioner of the Federal Acquisition Service (FAS). The following questions relate to this case.

- a. In Acting Administrator Tim Horne's response to the Office of Special Counsel concerning allegations raised by a whistleblower that were later substantiated, Horne noted that he instructed GSA's Senior Procurement Executive to review the existing delegations of procurement authority to TTS and determine whether any should be rescinded based on the reorganization.

- i. What is the current status?

As a part of the "Joining Forces" efforts GSA has examined multiple facets of integrating TTS into FAS, including a working group examining TTS acquisition activities. This working group is focused on the development, implementation and maturation of TTS acquisition internal controls through FY18 and beyond. GSA is taking a risk-based approach to procurement delegations under the direction of the Senior Procurement Executive which limits the number and type of procurement actions TTS can perform. FAS intends to leverage best practices as well as use enterprise-wide procurement processes, controls and systems in procurement as a baseline while allowing TTS to mature their procurement practices.

- ii. Have any delegations been rescinded? If so, which ones?

No delegations have been rescinded, however GSA reissued a new delegation to TTS in accordance with the plan outlined above on October, 18, 2017.

- b. The Inspector General investigation examined possible violation of the Anti-Deficiency Act that, ultimately, was determined an Economy Act violation. The IG reviewed allegations that 18F improperly managed Interagency Agreements by backdating agreements in violation of the Economy Act and found 101 of 18Fs 202 project agreements predated the execution of the an Interagency Agreement.

- i. How can such a large volume of agreements inappropriately be backdated?

18F began work on several engagements prior to signatures being executed due to lapses in internal controls and the desire to deliver services to agencies who needed work done quickly. This issue was

resolved through enhancing internal controls for teams beginning work for agencies. For example, 18F no longer begins work in advance of agreement signatures as a matter of both policy and practice per the controls mentioned in the response to question ii below.

- ii. What controls has GSA implemented to catch this type of systemic failure in the future?

GSA has documented and implemented a series of financial and management internal controls around the acceptance of Inter-Agency Agreements preventing the backdating of agreements. Below are a few of the specific internal controls now employed:

1. The Office of the Chief Financial Officer (OCFO) is now inserted into the agreement acceptance process. The last signature in the acceptance process of the agreement is made by the GSA OCFO. Additionally, a review and validation of the period of performance is done at that time.
2. System controls have been added to ensure all projects are linked to an appropriate funding source and billable work occurs only during the specified period of performance.
3. Monthly reconciliation processes have been instituted to ensure charges are properly allocated within the agreement period of performance, and that funds are available for billing/accrual purposes.

c. Have you personally reviewed the Inspector General's Investigative report on the recent GSA whistleblower reprisal case, specifically as it relates to TTS funding issues? Are you aware of any Anti-deficiency Act violations?

Yes, I have reviewed the report. No, I am not aware of Anti-deficiency Act violations.

d. Acting Special Counsel Adam Miles stated in his July 5, 2017 letter to the President and Congress that the reorganization of TTS may address concerns raised by the whistleblower case, but that "without additional details on improved management controls, the realignment does not address [the whistleblower's] substantiated concerns about mismanagement."

- i. What is FAS' specific plan for improving internal controls to ensure TTS has accurate revenue projections? What are the financial controls in place?

The Inspector General's evaluation of 18F's business operations was conducted from December 2015 through September 2016. Since then, TTS (18F's parent organization) has developed a corrective action plan in response to the IG report issued in October 2016 that addressed a number of financial and operating controls. They issued TTS-wide policy documents outlining these controls and communicated the changes to all employees.

GSA has implemented significant changes in the management approach for 18F to improve the operations of individual business units and TTS as a whole. In addition, TTS has implemented all the IG recommendations. We implemented all seven recommendations from “Evaluation of 18F.”¹ In addition, we implemented all six recommendations from “Evaluation of 18F’s Information Technology Security Compliance,”² including additional internal controls around hiring, revenue reconciliation and risk mitigation.

The program is monitoring the pipeline of actual and potential work orders to ensure that expenses are managed and workforce is utilized. Additional resources are only added if there is assurance of future work and capacity needs. Orders, pipeline, utilization and expenses are all closely monitored on a weekly and monthly basis. This process is a basis for the current plan to achieve full cost recovery.

As part of responding to the IG recommendations, TTS established new technical and procedural controls, including those related to when to begin billable project work and identifying funding sources at the beginning of engagements. TTS Policy for GSA Information FITARA Review requires GSA-CIO review and approval for all internal TTS contracts or agreements, as well as review and approval for external TTS contracts or agreements that leverage GSA IT platforms, security or infrastructure and conforms to GSA Policy 2101.1 CIO GSA Enterprise Information Technology Management (ITM) Policy. GSA has also developed extensive documentation of the TTS revenue generation, accrual, and reconciliation processes.

- ii. What is FAS' specific plan for improving internal controls to ensure TTS has sufficient and not inflated staffing levels?

Please see response directly above to 6(d)(i).

¹ JE17-001, Evaluation of 18F, issued 10/24/16.

² JE17-002, Evaluation of 18F’s Information Technology Security Compliance, issued 2/21/17.

Question for The Honorable Alan Thomas
Commissioner
General Services Administration, Federal Acquisition Service

**Questions for the Record from Rep. Gerald E. Connolly, Ranking Member Subcommittee on
Government Operations
House Committee on Oversight and Government Reform**

July 12, 2017, Hearing: "General Services Administration - Acquisition Oversight and Reform"

1. Are there currently any existing or pending government contracts between the government and the Trump Organization?

There are no active acquisition contracts with any entity associated with the Trump Organization above the micro-purchase threshold reported to Federal Procurement Data System (FPDS) in accordance with Federal Acquisition Regulation (FAR) Subpart 4.6 Contract Reporting.

2. Has the General Services Administration (GSA) taken any steps to protect against a conflict of interest that could arise from government contracts with businesses owned by the President of the United States, his family members, or his business partners? If so, please describe those steps.

GSA's responsibility is to ensure that the government receives the best value for the taxpayer and to ensure that all procurements adhere to the FAR and other relevant rules, regulations and statutes, including those that address conflict of interest.

3. Could the Acquisition Services Fund be used to purchase goods or services from a business in which President Trump has financial interests?

Every procurement action undertaken by GSA must be in compliance with the FAR and other relevant rules, regulations and statutes.

4. Has GSA delisted Kaspersky Labs from its approved vendor's list for information technology services and digital photographic equipment? Does this prevent agencies from using Kaspersky Labs' products or will they still be able to purchase these products through other means?

Kaspersky Lab (KL) was neither a Multiple Award Schedule (MAS) vendor, nor a contract holder, with the U.S. General Services Administration (GSA); therefore, there was never any contract or other agreement with KL for GSA to terminate. As you know, GSA recently became aware that KL products were available on the product lists of three MAS vendors -- A&T Marketing Inc., Federal Merchants Corp., and Bahfed Corp.; however, KL products were not included as part of A&T Marketing's 2015 or Federal Merchants' 2012 Schedule 70 contract awards, or Bahfed's 2013 Schedule 67 contract award. Again, the KL products were not added via required contract modification requests, but rather were improperly added via the Schedule Input Program (SIP), a proprietary software provided by GSA, that allows contractors to update commercial catalogs electronically on GSA Advantage!®.

On July 11, 2017, GSA directed all three vendors to remove KL products from their product lists, which all three vendors subsequently did. GSA is complying with the Binding Operational Directive, issued by the U.S. Department of Homeland Security on September 13, 2017, in regards to KL products.

5. If Kaspersky Labs has been delisted, will agencies that already use Kaspersky software be able to continue to use that software following GSA's action?

Currently, agencies' use of Kaspersky products is governed by DHS BOD 17-01, which has directed agencies to identify their use of Kaspersky products within 90 days and then begin to remove identified products from agencies systems.

6. If Kaspersky Labs has been delisted, is GSA continuing further actions against Kaspersky Labs?

GSA did not have a contractual relationship with Kaspersky Lab and no further action is planned by GSA.

7. Section 4 of Executive Order 13-360 in 2004 directed GSA to establish a Government Wide Acquisition Contract (GWAC) at the agency. The purpose was to help Federal agencies meet their 3% goal of contracting with Service Disabled Veteran Owned Small businesses. This became known as the Veterans Technology Services (VETS) GWAC, or the VETS GWAC. On February 2, 2007, the VETS GWAC was awarded to forty-three (43) SDVOSBs and administered by the GSA Heartland Region 6 in Kansas City, MO with a base period of five years, expiring on February 1, 2012. On February 2, 2012, the first and only five-year option period was then awarded to qualified contract holders i.e. those initial contract holders that 1.) produced adequate revenue and 2.) had not grown revenue to exceed the \$27.5 million NAICS Code 541512 threshold. This contract expired with the end of the option period on February 1, 2017. On April 21, 2016, the GSA issued a solicitation for a replacement to the VETS GWAC contract, with a short name of VETS2 GWAC. Bids were submitted on June 18, 2016 and as of today, there have been no contracts awarded to replace the original contracts.

When does GSA intend to execute the replacement contract? Why has the replacement contract been so delayed? What is the timeline for an expected award of the replacement contract? Since the option period ended February 1, 2017 and the replacement contract has not been put into place, does that mean that all FY2017 opportunities have been are lost? If so, what is the dollar figure for lost SDVOSB opportunities since GSA did not have a replacement contract in place between June 2016 and February 2017 and what is the dollar figure for lost opportunities in FY2018?

GSA regrets not awarding VETS 2 contracts before the VETS GWAC expired. However, by taking the time to obtain industry and customer input, GSA believes that it has developed an improved VETS GWAC that will provide increased access to SDVOSBs. GSA understands the importance of the VETS 2 GWAC to the Service-Disabled Veteran-Owned Small Business (SDVOSB) community and is expediting its evaluation of proposals. The Solicitation was issued on April 21, 2016 and closed on June 20, 2016. GSA received over 175 proposals to review and evaluate.

On August 22, 2017 GSA published the required pre-award notice for small business programs in FedBizOpps, announcing that evaluations were complete and listing the apparent successful offerors. On October 26, 2017, GSA announced the award of the VETS 2 contracts to 70 SDVOSB firms.

Lost business volume for the next fiscal year is projected to be very low as there are several alternative contract vehicles available including GSA Schedule 70, NASA SEWP and VA's T4 Next Generation

(T4NG) contract. In addition, agencies can conduct set aside acquisitions using Alliant Small Business and STARS 2 and GSA offers assistance to agencies in using alternative solutions. Obligated dollars through IT Schedule 70 to SDVOSBs over the previous fiscal years is \$687.7M in FY 15, \$740.3M in FY 16 and \$795.3M in FY17.

8. FedRAMP has made significant progress over the past year and a half. Cloud service providers are more prepared to go through the Authorization to Operate (ATO) process and the ATO process timeline has been reduced from 18-24 months down to an average of four months. What steps does GSA plan to take to continue to improve the FedRAMP program? How does stakeholder engagement fit into GSA's plans to improve FedRAMP?

First, GSA will continue to ensure that all JAB authorization decisions occur in less than 6 months so that no authorization effort will take longer than 6 months. This commitment to timeline was a direct output of the FedRAMP Accelerated initiative that began in FY16.

Second, GSA released a FedRAMP Tailored Baseline requirements for Low Impact Software as a Service. The requirements for this baseline are reduced from 126 down to 36 and has a reduced set of documentation requirements as well. It's expected that authorizations under this process could happen in as quickly as 4-6 weeks. The Tailored Baseline requirements are designed for low risk cloud solutions that many digital service teams and agencies either currently use or have a need to use - tools that focus on collaboration, project management, and open source development and public engagement.

Similar to the redesign efforts that FedRAMP undertook to reduce the authorization timelines via FedRAMP Accelerated and FedRAMP Tailored, FedRAMP is doing the same thing for the ongoing efforts associated with Continuous Monitoring once systems get authorized. Although much attention is given to the initial assessment, the Continuous Monitoring by FedRAMP of Cloud Service Providers is significant, with monthly reviews of vulnerabilities and yearly assessments, as well as reviewing changes to systems after authorization. FedRAMP just finished the research phase of this effort by working with a broad range of vendors and agencies to understand capabilities and needs. The design and implementation phase is just getting underway and is expected to be completed by the end of FY18. FedRAMP believes that this effort can help reduce the level of effort for government and vendors by anywhere from 25%-50%.

GSA is also looking at ways to automate portions of FedRAMP - from process and business flow, to creating machine-readable formats for all of the templates and so that agencies can use whatever tools they have in place currently to help them automate the authorization process. This includes partnering with industry tool vendors on how to best promote interoperability, with over 40 respondents to a recent request for information.

The voice of the customer and stakeholder engagement is at the heart of all of the major initiatives that FedRAMP undertakes. FedRAMP completes post authorization surveys with every vendor, and has regular check-ins with vendors on how FedRAMP can improve. GSA also releases an annual survey where, in the most recent version, 82% of respondents had a favorable rating of the program, and all major changes to the policy or requirements go through two rounds of public comment before being finalized to ensure we hear from all stakeholders on the impact and feasibility of any changes.

9. What is GSA doing to help agencies improve their FITARA Scorecard performance on data

center consolidation?

GSA's Data Center Optimization Initiative Program Management Office (PMO) serves as a resource to help agencies implement DCOI optimization plans by facilitating participation in interagency data center shared services; sharing best practices and information about tools for improving data center efficiency; and supporting agencies reporting on progress toward FITARA goals. The Data Center PMO mission and goals reflect its role in carrying out DCOI policy by establishing a customer-centric approach to empowering agencies to meet optimization and efficiency goals. The Data Center PMO's mission is to define, design, implement, and monitor a set of government-wide IT infrastructure solutions which leverage data center community input.

10. How is GSA currently evaluating any supply chain concerns, including foreign ownership and influence, or foreign investment, in contractors seeking to get onto federal government contract vehicles?

GSA has implemented numerous supply chain risk management strategies and GSA continues to further explore additional opportunities, particularly through interagency groups and partnerships with other agencies. Some specific examples of GSA efforts include:

- Contractors are required to make representations and certifications through FAR Clause 52.212-3 when completing the award process on GSA contract vehicles. Through this clause contractors represent whether they are a foreign entity, whether they are an inverted domestic corporation, the place of manufacturer, compliance with Trade Agreements Act and Buy American Act as applicable. GSA Contracting Officers rely on these representations and certifications in making responsibility determinations prior to award of contract.
- During contract administration, GSA engages in a number of supply chain risk management activities such as utilizing data analytics to identify product authenticity and utilizes Industrial Operational Analysts to review contractor compliance with requirements such as providing Trade Agreement Act compliant products through the Multiple Award Schedules (MAS) program. When GSA Contracting Officers are informed through data, Industrial Operations Analysts or other sources on potential non-compliance they take appropriate contract action to address compliance with contractual requirements.

Question for The Honorable Alan Thomas
Commissioner
General Services Administration, Federal Acquisition Service

Questions for the Record from Rep. Stephen F. Lynch Subcommittee on Government Operations
House Committee on Oversight and Government Reform

July 12, 2017, Hearing: "General Services Administration - Acquisition Oversight and Reform"

1. A provision of the National Defense Authorization Act for fiscal year 2018 would require the Administrator of GSA to establish a program for the procurement of commercial goods through online marketplaces.

One section of the online marketplace provision states that the award of a contract to the marketplace provider or providers -the entities establishing the online purchasing sites - "may be made without the use of full and open competition."

Full and open competition, with certain limited exemptions, has been the gold standard in federal procurement since passage of the Competition in Contracting Act in 1984.

Competition helps to ensure that the government receives the best value for the American taxpayer.

- a. If this provision were to become law, would GSA use full and open competition to award the online marketplace provider contracts? If not, how would you ensure that taxpayers receive the best value?

Competition is a guiding principle in our procurement system as stated in the Federal Acquisition Regulation. GSA intends to use competition in the selection of platform providers, unless an enumerated statutory exception to competition is justified. Based on its current understanding of the market, GSA believes competition is the ideal avenue to achieve best value for the Government and the taxpayer and does not envision a specific scenario where an exception would be invoked.

2. The federal government has invested considerable resources into existing online ordering programs, like the Federal Supply Schedules and Defense Department's FedMall. The online marketplace provision established by the NDAA would seem to be in direct competition with those existing programs. Please answer the following :

- a. What impact do you think the provision would have on the existing programs?

GSA is looking at opportunities to streamline access to the federal market for vendors and simplify procurement for agencies, mirroring how taxpayers purchase in the commercial world. As a part of this implementation, GSA would implement a commercial platform in a considered and phased roll-out.

GSA intends to implement the enacted provision (section 846 of the FY 18 NDAA), in concert with ongoing initiatives, to ensure the best use of taxpayer dollars and efficient technology tools.

- b. The NDAA proposal would allow for decentralized purchasing. How would this align with current federal purchasing programs like Strategic Sourcing and Category Management?

The Section 846 language aligns well with the fundamental principles of strategic sourcing and category management. In particular, section 846 anticipates that platforms which are part of the program would capture data on the purchases to provide visibility into those purchases and allow agencies to evaluate and compare results (e.g., pricing, small business participation, other considerations) from different acquisition strategies, including decentralized purchasing vs. coordinated purchases through category management. This discretion is reinforced by section 846(b), which makes clear that use of the authority is discretionary and not intended to displace other authorities (which would include buying strategies) whose use would be more appropriate. and Section 846(c)(2)(C), which requires GSA and OMB to conduct an assessment of the products or product categories that are suitable for purchase on the commercial e-commerce portals as part of the phase II report that is due to Congress in March 2019.

- c. How does GSA propose to reconcile the NDAA's proposed language, which would prohibit modification of the online marketplace's terms and conditions, with the existing unique government requirements for purchasing?

GSA is meeting with key stakeholders regarding the implementation of NDAA section 846 including vendors of e-commerce platforms, industry providers to the federal government, customer agencies as well as the oversight community to determine the best way forward. The first listening session was held on January 9, 2018. GSA is now reconciling comments from that feedback session. In particular, GSA recognizes that there are some differences between online marketplace terms and conditions and existing government requirements. Through ongoing active agency and industry outreach, GSA will gain a deep understanding of government agency requirements and of portal providers' terms and conditions. This knowledge will help inform the phase II report, due to Congress in March 2019.

Questions for The Honorable Rob Cook

Deputy Commissioner (Director, Technology Transformation Services)
Federal Acquisition Service

**Questions for the Record from Chairman Will Hurd Subcommittee
on Information Technology
House Committee on Oversight and Government Reform**

July 12, 2017, Hearing: "General Services Administration -Acquisition
Oversight and Reform"

-
1. In August 2016, a GAO report (GAO-16-602) made two recommendations to GSA related to 18F. Has 18F implemented GAO's recommendations?

TTS has developed outcome oriented program goals and associated performance measures for 18F to include cost recovery metrics. The FAS Commissioner, the Chief Financial Officer and the TTS Director review 18F performance measures and cost recovery on a regular basis.

- a. If not, when do you expect to implement these recommendations? N/A

2. What percentage of 18F employees have been hired via Schedule A authority?

Currently, 89% of 18F staff were hired via the Schedule A Authority.

3. Do you see 18F continuing to grow in size or staying where it is now?

18F began FY 2017 with a staff of 169, and has decreased in size during the year, finishing FY 2017 with a staff of 123. During FY 2018, we are planning steady staffing of approximately 150. 18F has adjusted its management approach to ensure that staff size correlates to demand and is working closely with the GSA CFO to ensure that growth does not outpace business volume.

- a. Will the percentage of Schedule A positions increase, decrease, or stay the same?

We continue to seek the best mix of Schedule A and competitively hired permanent employees to attain the strongest mix of technical skills to continue helping the federal government modernize its information technology.

4. When do you project 18F will achieve full cost recoverability?

In response to the corrective action plan issued as a result of the Inspector General reports, TTS is moving as quickly as possible in the direction of full cost recovery and expects to

achieve full cost recovery in fiscal year 2019. For instance, in conjunction with FAS leadership, 18F is making operational adjustments, such as increasing staff utilization rates, to achieve cost recovery.

5. Are there controls in place to measure and ensure that the work 18F is performing is targeted to recover its costs?

Yes. 18F takes cost recovery seriously. We have made operational improvements and developed controls to manage financial success. 18F analyzes its cost recovery and sales pipeline weekly. TTS, 18F's home organization, works closely with the CFO's office to reconcile billing monthly and conducts monthly financial reviews with the CFO and TTS leadership.

6. The Federal Risk and Authorization Management Program (FedRAMP) is a GSA led government-wide program to certify the cybersecurity of cloud products and services. This Committee would like to ensure that administrative hurdles to widespread adoption of cloud solutions are minimal and security of such solutions is sufficient. Certain stakeholders and media reports have indicated that the GSA's FedRAMP process takes too long and is too costly.¹

- a. What is the average time it takes a cloud services provider to clear the FedRAMP process?

The FedRAMP Program Management Office at GSA has worked over the last 18 months to drastically reduce the time it takes to achieve an authorization through the Joint Authorization Board. Through that work the timing was reduced by 75% to approximately 12-16 weeks for an Authority to Operate (ATO) decision, down from an average of 18 months.

- b. Typically, what are the causes of delays in obtaining FedRAMP certification?

The typical causes for a delay center around the vendor not having all the correct technical security controls fully implemented, in particular: multi-factor authentication, Federal Information Processing Standard (FIPS) and NIST validated encryption, and configuration management and vulnerability management (e.g. resolving vulnerabilities in a timely manner). Industry reports that FIPS assessments, which are mandated by law (e.g., not FedRAMP program) can often take upwards of 16-24 months.

To help clarify these expectations, FedRAMP released a rapid FedRAMP Readiness process for vendors to work with industry auditors and third party assessors to ensure that they have all of the key technical pieces in place before beginning a FedRAMP assessment. To date, over 30 vendors have actively participated in this readiness process as they build out their service to ensure they have the key technical pieces in place to achieve a FedRAMP authorization.

- c. How much does it cost for a cloud service provider to go through the FEDRAMP process? Please provide the high and low range of such costs and any information indicating how these costs have changed over time.

One company (Coalfire Federal) recently completed research³ around the costs associated with obtaining a FedRAMP authorization and found them to be between \$350,000 and \$865,000 depending on a cloud provider's readiness, overall complexity, and pre-assessment activities. Clearly, large vendors providing government-wide platforms can require more investment, but we're continuing to drive this cost down by redesigning processes and leveraging the potential for automation.

The Coalfire study found that the costs associated with achieving a FedRAMP authorization was comparable to other compliance regimes such as Service Organization Control (SOC) II, Payment Card Industry Data Security Standard (PCI DSS), and International Standards Organization (ISO) 270001.

- d. How many agencies currently use FEDRAMP certified products and services?

There are over 120 agencies working with FedRAMP - this includes agencies in all three branches of government - Executive, Judicial, and Legislative

- e. How can the FEDRAMP process be improved?

We're continually looking for ways to improve the process, and some of our most recent work has been partnering with industry to identify ways to streamline the continuous monitoring aspect of FedRAMP. Most people consider the upfront assessment, and don't realize that we conduct monthly reviews with each provider to ensure they maintain high levels of security standards, such as patching high-security vulnerabilities within 30 days. This means that the government makes a long-term commitment in promoting the security of critical internet-based companies, often benefiting commercial institutions that leverage these same providers. As a small organization, we continue to re-evaluate how we allocate costs and work with our industry partners to streamline the security review and oversight processes.

Additionally, GSA released a FedRAMP Tailored Baseline requirements for Low Impact Software as a Service. The requirements for this baseline are reduced from 126 down to 36 and has a reduced set of documentation requirements as well. It's expected that authorizations under this process could happen in as quickly as 4-6 weeks. The Tailored Baseline requirements are designed for low risk cloud solutions that many digital service teams and agencies either currently use or have a need to use - tools that focus on

³ <https://www.coalfire.com/The-Coalfire-Blog/May-2017/Meeting-FedRAMP-Standards-Report>

collaboration, project management, and open source development and public engagement.

- f. Are there potential improvements that may be realized through legislation?

We believe that improvements to the security processes that secure and safeguard our Federal infrastructure are strongly tied to IT modernization activities. We appreciate the committee's oversight of this subject, and we believe continued dialogue around the topic is critical. For FedRAMP specifically, it's largely a voluntary requirement for agencies, and a recent study by Deltek- plus positive media impressions⁴ showed that vendors continue to recognize the value of FedRAMP certification and the improvements to the program. Continued legislative attention on IT modernization and security, in partnership with other key Federal stakeholders, can help the program increase value over time.

7. On May 17, 2017, the House passed the Modernizing Government Technology Act (H.R. 2227). This legislation is designed to incentivize federal agencies and CIOs to transition from legacy systems to modern, more secure systems, including cloud solutions. The bill also assigns a significant role to GSA related to the centralized Technology Modernization Fund.

- a. What expertise will GSA bring to fulfill the MGT Act objective of modernizing federal government IT?

GSA will bring a range of expertise and resources to help achieve the goals of the Act. For example, within the Federal Acquisition Service, TTS has in-house technical and product experts, who can help ensure that investments through the Technology Modernization Fund are focused on delivery. Within FAS more broadly, GSA has significant procurement expertise to help ensure that agencies receive the best-in-class from industry and service providers. Finally, as a centralized shared-service provider within the federal government, GSA is uniquely positioned to offer shared services and platforms to enable agencies to reduce the number of duplicative legacy systems.

- b. What work is GSA and specifically TTS currently doing to modernize federal IT government-wide? Please provide a sampling of such projects and cost savings realized.

TTS has a number of mature offerings within the Office of Products and Programs (OPP), such as FedRAMP, api.data.gov, the Digital Analytics Program, and the USAGov Contact Center, that collectively save an estimated \$100 million annually. Additionally, 18F has saved agencies millions of dollars through its consulting work and its main production product offering, cloud.gov. For example, the Federal Election Commission has reported that

⁴ Positive press samples: <https://goo.gl/s29U4D>, <https://goo.gl/DkvQit>, <https://goo.gl/wp6HmC>

it will be able to reinvest \$1.2 million annually by using cloud.gov. Finally, through authorities granted by the Intergovernmental Cooperation Act, the TTS Office of Acquisition has helped multiple federal and state agencies modernize legacy systems, with substantial cost avoidance and savings, and faster delivery cycles.

8. The Committee is concerned that the Government may be developing products that compete with the private sector, and waste government resources when a commercial alternative is available.

- a. For example, why did 18F build cloud.gov?

Current infrastructure and platform solutions available to government do not have built-in compliance and security measures that address federal guidelines. As 18F was building IT solutions for agencies, we did not have a way to quickly access infrastructure without building costly and time consuming custom solutions on top of it. We saw a deep need for modern infrastructure that would reduce the time to delivery, especially reducing the effort associated with developing solutions within government regulations and security considerations.

- b. Does cloud.gov compete with private sector providers?

- c. When cloud.gov first launched, GSA's intent was to assist federal agencies in delivering citizen-facing services in a faster, more user-centered way. As GSA has worked with its industry partners and customers to better understand cloud hosting needs, the cloud.gov model has matured and evolved to better recognize the changes and advancements made by the private sector in this space. It remains GSA's intent that, to the greatest extent possible, cloud.gov should not compete with private sector providers when solutions that adequately address government-specific needs are available. To help ensure this, it is GSA's plan moving forward to use cloud.gov as a way to deploy prototypes and create appropriate templates and standards for open source federal hosting, similar to a sandbox. GSA will work closely with its customers, when ready for full production, to source and procure the appropriate cloud hosting environment from among commercially available options. What procedures are in place to ensure GSA is selecting commercially available IT solutions (Buy vs Make) in compliance with the Clinger Cohen Act, FITARA and OMB A130 reporting?

GSA firmly believes that government should build solutions only when a private sector solution is unable to meet government demands. In carrying out that principle, GSA ensures all IT acquisitions are in compliance with federal policies, regulations and statutes. There are controls in place at GSA to ensure IT acquisitions follow long-established acquisition procedures. All IT purchases for systems operated by GSA are reviewed and approved by the GSA CIO as required by FITARA and OMB policy. The cloud.gov platform, in particular, is underpinned by a variety of products and services purchased from the commercial marketplace. For instance, TTS currently purchases AWS infrastructure from a Service-Disabled Veteran-Owned Small Business (SDVOSB) reseller and the platform uses many other private sector Software-as-a-Service tools, such as PagerDuty.

9. In your testimony, you mentioned 18F's role in assisting Treasury with implementing the DATA Act, but didn't mention 18F's role helping OMB implement the DATA Act's procurement pilot for recipient reporting.

- a. Please describe 18F's past/current role in the procurement pilot?

The 18F team focused on prototyping potential solutions for reducing contractor burden and evaluating their viability through user research and testing. The learnings generated by prototyping were presented to GSA's Office of Governmentwide Policy to inform the development of a production model that may be piloted.

- b. Who was primarily responsible for implementing the procurement pilot?

The Office of Management and Budget's Office of Federal Procurement Policy (OFPP) was responsible for the strategic direction and management of the pilot with GSA managing the design, development, and delivery of the technology solution.

- c. When was GSA first approached to work with OMB on the pilot?

18F was first approached in March 2015.

- d. How many contractors participate in the pilot?

One contractor, NuAxis, built the pilot system.

- e. The procurement pilot focuses on Davis-Bacon reporting (on payment of prevailing wages). How was Davis-Bacon reporting selected? Why made this decision?

The initial reporting requirement for the tool is the method by which contractors certify their proper payment of prevailing wages as required by the Department of Labor's regulations implementing the Davis-Bacon Act (See 29 CFR 3.3, 5.5(a)(3)). The recently released OMB report on the pilot outlines in detail how OMB selected these areas. The idea was to prototype a tool to simplify the reporting process to enable contractors to remain in compliance with these regulations while reducing reporting burden.

10. The Committee understands 18F may have done projects for state governments. The Committee is concerned that this effort and associated resources could be better spent addressing IT challenges within the federal government.

- a. Please describe the work 18F may be doing for state governments, by project, cost and dates.

18F is working with state governments via the authority provided in the Intergovernmental Cooperation Act (IGCA). Like many federal agencies, state and local governments face enormous IT challenges and every year receive billions of dollars in federal grant funds to modernize and improve their IT systems.

When work is linked to federal projects/funding, the 18F Acquisition team collaborates with both federal and state/local partners to help states responsibly spend federal grant money by providing acquisition and technical consulting for improving state IT systems. Active projects are:

- **State of California**
 - Medicare and Medicaid enrollment and eligibility (not to exceed \$350,000 through 6/30/2018)
 - Child welfare systems (not to exceed \$575,000.00 through 6/30/2018)
- **State of Alaska:**
 - Medicare and Medicaid enrollment and eligibility (not to exceed \$1,770,000 through 6/30/2018)
 - Child welfare systems (not to exceed \$300,000 through 6/30/18)
- **State of Vermont**
 - Medicare and Medicaid enrollment and eligibility (not to exceed \$1,000,000 through 6/30/2018)

b. Does 18F plan to continue work for state and/or local governments?

When linked to federal projects/funding, 18F will work with state and local governments in order to help states responsibly spend federal grant money dedicated to IT modernization. We will only undertake those projects on a fully-reimbursable basis and in compliance with all applicable statutes and regulations.

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<http://oversight.house.gov>

August 30, 2017

Alan Thomas, Commissioner
Federal Acquisition Service
U.S. General Services Administration
1800 F Street, N.W.
Washington, D.C. 20006

Dear Commissioner Thomas:

Enclosed are post-hearing questions that have been directed to you and submitted to the official record for the hearing that was held on July 12, 2017, titled "General Services Administration – Acquisition Oversight and Reform."

In order to ensure a complete hearing record, please return your written response to the Committee on or before September 13, 2017, including each question in full as well as the name of the Member. Your response should be addressed to the Committee office at 2157 Rayburn House Office Building, Washington, DC 20515. Please also send an electronic version of your response by e-mail to Kiley Bidelman, Clerk, at Kiley.Bidelman@mail.house.gov.

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Julie Dunne at (202) 225-5074.

Sincerely,



Mark Meadows
Chairman
Subcommittee on Government Operations



Will Hurd
Chairman
Subcommittee on Information Technology

Enclosure

Questions for The Honorable Alan Thomas

Commissioner
General Services Administration, Federal Acquisition Service

Questions for the Record from Chairman Mark Meadows Subcommittee on Government Operations House Committee on Oversight and Government Reform

July 12, 2017, Hearing: "General Services Administration – Acquisition Oversight and Reform"

1. What do you see as GSA's best opportunity to streamline federal acquisition?
2. How does GSA ensure the federal acquisition process reflects commercial best practices, including reasonable pricing in acquisition vehicles, such as GSA schedule contracting?
3. How many Federal Acquisition Regulation (FAR) and General Services Acquisition Regulation (GSAR) clauses apply for the acquisition of commercial goods and services? Please provide a list with title and cite for the clause.
4. How will you use GSA's membership on the FAR Council to assess the current FAR and reduce the regulatory/compliance costs for federal contractors?
5. Currently, what services/tools does FAS provide to other agencies to assist with IT modernization and acquisition?
6. On July 6, 2017, GSA settled a whistleblower case brought by former Commissioner of the Federal Acquisition Service (FAS). The following questions relate to this case.
 - a. In Acting Administrator Tim Horne's response to the Office of Special Counsel concerning allegations raised by a whistleblower that were later substantiated, Horne noted that he instructed GSA's Senior Procurement Executive to review the existing delegations of procurement authority to TTS and determine whether any should be rescinded based on the reorganization.
 - i. What is the current status?
 - ii. Have any delegations been rescinded? If so, which ones?
 - b. The Inspector General investigation examined possible violation of the Anti-Deficiency Act that, ultimately, was determined an Economy Act violation. The IG reviewed allegations that 18F improperly managed Interagency Agreements by backdating agreements in violation of the Economy Act and found 101 of 18Fs 202 project agreements predated the execution of the an Interagency Agreement.
 - i. How can such a large volume of agreements inappropriately be backdated?

- ii. What controls has GSA implemented to catch this type of systemic failure in the future?
- c. Have you personally reviewed the Inspector General's Investigative report on the recent GSA whistleblower reprisal case, specifically as it relates to TTS funding issues? Are you aware of any Anti-deficiency Act violations?
- d. Acting Special Counsel Adam Miles stated in his July 5, 2017 letter to the President and Congress that the reorganization of TTS may address concerns raised by the whistleblower case, but that "without additional details on improved management controls, the realignment does not address [the whistleblower's] substantiated concerns about mismanagement."
 - i. What is FAS' specific plan for improving internal controls to ensure TTS has accurate revenue projections? What are the financial controls in place?
 - ii. What is FAS' specific plan for improving internal controls to ensure TTS has sufficient and not inflated staffing levels?

Question for The Honorable Alan Thomas
Commissioner
General Services Administration, Federal Acquisition Service

Questions for the Record from Rep. Gerald E. Connolly, Ranking Member
Subcommittee on Government Operations
House Committee on Oversight and Government Reform

July 12, 2017, Hearing: "General Services Administration – Acquisition Oversight and Reform"

1. Are there currently any existing or pending government contracts between the government and the Trump Organization?
2. Has the General Services Administration (GSA) taken any steps to protect against a conflict of interest that could arise from government contracts with businesses owned by the President of the United States, his family members, or his business partners? If so, please describe those steps.
3. Could the Acquisition Services Fund be used to purchase goods or services from a business in which President Trump has financial interests?
4. Has GSA delisted Kaspersky Labs from its approved vendor's list for information technology services and digital photographic equipment? Does this prevent agencies from using Kaspersky Labs' products or will they still be able to purchase these products through other means?
5. If Kaspersky Labs has been delisted, will agencies that already use Kaspersky software be able to continue to use that software following GSA's action?
6. If Kaspersky Labs has been delisted, is GSA continuing further actions against Kaspersky Labs?
7. Section 4 of Executive Order 13-360 in 2004 directed GSA to establish a Government Wide Acquisition Contract (GWAC) at the agency. The purpose was to help Federal agencies meet their 3% goal of contracting with Service Disabled Veteran Owned Small businesses. This became known as the Veterans Technology Services (VETS) GWAC, or the VETS GWAC. On February 2, 2007, the VETS GWAC was awarded to forty-three (43) SDVOSBs and administered by the GSA Heartland Region 6 in Kansas City, MO with a base period of five years, expiring on February 1, 2012. On February 2, 2012, the first and only five-year option period was then awarded to qualified contract holders i.e. those initial contract holders that 1.) produced adequate revenue and 2.) had not grown revenue to exceed the \$27.5 million NAICS Code 541512 threshold. This contract expired with the end of the option period on February 1, 2017. On April 21, 2016, the GSA issued a solicitation for a replacement to the VETS GWAC contract, with a short name of VETS2 GWAC. Bids were submitted on June 18, 2016 and as of today, there have been no contracts awarded to replace the original contracts.

When does GSA intend to execute the replacement contract? Why has the replacement contract been so delayed? What is the timeline for an expected award of the replacement contract? Since the option period ended February 1, 2017 and the replacement contract has not been put into place, does that mean that all FY2017 opportunities have been are lost? If so, what is the dollar figure for lost SDVOSB opportunities since GSA did not have a replacement contract in place between June 2016 and February 2017 and what is the dollar figure for lost opportunities in FY2018?

8. FedRAMP has made significant progress over the past year and a half. Cloud service providers are more prepared to go through the Authorization to Operate (ATO) process and the ATO process timeline has been reduced from 18-24 months down to an average of four months. What steps does GSA plan to take to continue to improve the FedRAMP program? How does stakeholder engagement fit into GSA's plans to improve FedRAMP?
9. What is GSA doing to help agencies improve their FITARA Scorecard performance on data center consolidation?
10. How is GSA currently evaluating any supply chain concerns, including foreign ownership and influence, or foreign investment, in contractors seeking to get onto federal government contract vehicles?

Question for The Honorable Alan Thomas
Commissioner
General Services Administration, Federal Acquisition Service

Questions for the Record from Rep. Stephen F. Lynch
Subcommittee on Government Operations
House Committee on Oversight and Government Reform

July 12, 2017, Hearing: “General Services Administration – Acquisition Oversight and Reform”

1. A provision of the National Defense Authorization Act for fiscal year 2018 would require the Administrator of GSA to establish a program for the procurement of commercial goods through online marketplaces.

One section of the online marketplace provision states that the award of a contract to the marketplace provider or providers – the entities establishing the online purchasing sites – “may be made without the use of full and open competition.”

Full and open competition, with certain limited exemptions, has been the gold standard in federal procurement since passage of the Competition in Contracting Act in 1984. Competition helps to ensure that the government receives the best value for the American taxpayer.

- a. If this provision were to become law, would GSA use full and open competition to award the online marketplace provider contracts? If not, how would you ensure that taxpayers receive the best value?
2. The federal government has invested considerable resources into existing online ordering programs, like the Federal Supply Schedules and Defense Department’s FedMall. The online marketplace provision established by the NDAA would seem to be in direct competition with those existing programs. Please answer the following:
 - a. What impact do you think the provision would have on the existing programs?
 - b. The NDAA proposal would allow for decentralized purchasing. How would this align with current federal purchasing programs like Strategic Sourcing and Category Management?
 - c. How does GSA propose to reconcile the NDAA’s proposed language, which would prohibit modification of the online marketplace’s terms and conditions, with the existing unique government requirements for purchasing?

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<http://oversight.house.gov>

July 22, 2016

The Honorable Denise Turner Roth
Administrator
General Services Administration
1800 F Street, NW, Room 6120
Washington, D.C. 20405

Dear Administrator Roth:

The federal government's Computers for Learning (CFL) program enables schools and educational non-profit organizations to obtain excess computer equipment from federal agencies. The program distributes nearly 30,000 pieces of computer equipment to schools and non-profits each year.¹ According to a recent media report, the CFL program is potentially vulnerable to misuse and criminal activity.²

The General Services Administration manages the platform, GSAXcess, which federal agencies use to convey excess property, including computers and peripheral equipment, to schools and educational non-profit organizations through the CFL program.³ In light of the Committee's recent findings about the GSAXcess platform, we are concerned the CFL program suffers from the same vulnerabilities as GSA's Surplus Firearm Donation Program, which exposed government firearms to loss and theft.⁴ The fact that two programs that donate surplus government property face similar risks related to GSAXcess raises questions about the viability of this platform for donation purposes.

The report also raised concerns about management of the CFL program. The report stated "there is no government-wide requirement of background checks or in-person visits of

¹ Scott MacFarlane *et al.*, Federal Computers Intended for Donation to Public Schools Stolen in Fraud Schemes, NBC 4 I-Team, June 30, 2016, available at <http://www.nbcwashington.com/investigations/Federal-Computers-Intended-for-Donation-to-Public-Schools-Stolen-in-Fraud-Schemes-385107041.html>. [hereinafter MacFarlane]

² *Id.*

³ General Services Administration website, "Computers for Learning Program," available at <https://computersforlearning.gov/> (last visited July 13, 2016).

⁴ Gen. Services Admin. Office of Inspector Gen., *Limited Evaluation of GSA Surplus Firearm Donation Program: Inadequate Controls May Leave Firearms Vulnerable to Theft, Loss, and Unauthorized Use* (June 12, 2015) (JE15-004), available at <https://www.gsaig.gov/content/limited-evaluation-gsa-surplus-firearm-donation-program-inadequate-controls-may-leave>. See also, *Firearms Lost: GSA's Administration of the Surplus Firearm Donation Program: Hearing before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Mar. 2, 2016).

schools or non-profit agencies that apply for equipment to the program. There is also no ban on recipients re-selling the computers they obtain through Computers for Learning.”⁵

Investigations by multiple law enforcement organizations produced evidence of fraud schemes designed to take advantage of the lax oversight of the CFL program.⁶ For example, a man in California was able to pose as a member of 14 different non-profit organizations between 2007 and 2013 to obtain computers for free through the CFL program.⁷ He then sold the computers for personal profit. Throughout the course of this scheme, the man obtained 19,442 items and sold them for \$7.2 million.⁸ This individual was ultimately prosecuted and sentenced to ten years in prison.⁹

It is imperative that GSA takes immediate steps to address mismanagement of the CFL program. This is just one example where lax program oversight allowed criminals to steal from CFL, which was designed to benefit schoolchildren. The agency must ensure that the excess computer equipment ends up in the hands of the children for whom it was intended.

Toward that end, please provide the following documents and information as soon as possible, but no later than August 5, 2016:

1. Documents referring or relating to GSA’s responsibilities for supporting the CFL program, including, but not limited to, the number of staff that support the CFL program, the annual cost of supporting the CFL program, and a representative sample of any interagency agreements with federal agencies;
2. Documents sufficient to describe the donation process to a school or non-profit organization through the CFL program, including, but not limited to, any forms used to verify eligibility of schools and non-profit organizations;
3. Documents and communications referring or relating to processes to verify that computers and peripheral equipment are going to the intended recipients and used for an appropriate purpose;
4. Documents sufficient to show the final disposition of all computers and peripheral equipment transferred through the CFL program, including, but not limited to, the name and location of the final eligible recipient, process for destruction of unclaimed equipment, and records of all destroyed equipment;

⁵ MacFarlane, *supra* note 1.

⁶ United States Attorney’s Office, Western District of Washington press release “California Man Who Fraudulently Obtained and Sold Computers Destined For Schools and Non-Profits Sentenced To 10 Years In Prison” (Feb. 5, 2015), *available at* <https://www.gsaig.gov/news/california-man-who-fraudulently-obtained-and-sold-computers-destined-schools-and-non-profits>. [hereinafter U.S. Attorney’s Office Press Release]

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

The Honorable Denise Turner Roth

July 22, 2016

Page 3

5. Documents and communications referring or relating to any steps GSA has taken toward conducting a program-wide inventory of all computers and peripheral equipment transferred to schools and non-profit organizations between 2010 and 2015;
6. Documents and communications referring or relating to periodic audits of any recipient's eligibility to receive computer and peripheral equipment through the CPL program; and
7. Documents and communications referring or relating to procedures for scrubbing computer equipment before transfer.

When producing documents to the Committee, please deliver production sets to the Majority staff in room 2157 of the Rayburn House Office Building and the Minority staff in room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment to this letter provides additional information about responding to the Committee's request.

The Committee on Oversight and Government Reform is the principal oversight committee in the U.S. House of Representatives. Pursuant to House Rule X, the Committee has authority to investigate "any matter" at "any time."

Please contact Kevin Ortiz of the Majority staff at (202) 225-5074 with any questions about this request. Thank you for your attention to this matter.

Sincerely,



Jason Chaffetz
Chairman



Mark Meadows
Chairman
Subcommittee on
Government Operations

Enclosure

cc: The Honorable Elijah E. Cummings, Ranking Member

The Honorable Gerald E. Connolly, Ranking Member
Subcommittee on Government Operations

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
 - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
 - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,
CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE,
DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,
INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.
6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.
17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.

19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.
3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term "identify," when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term "referring or relating," with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term "employee" means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.



Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

March 24, 2016

Christopher P. Bertram, Staff Director

Katherine W. Dedrick, Democratic Staff Director

Mr. Norman Dong
Commissioner
Public Buildings Service
U.S. General Services Administration
1800 F Street, NW
Washington, D.C. 20405

Dear Commissioner Dong:

Thank you for your testimony before the Subcommittee on Economic Development, Public Buildings, and Emergency Management at the hearing entitled "Saving Taxpayer Dollars by Reducing Federal Office Space Costs," held on March 1, 2016. As a follow-up to that hearing, attached, please find questions submitted for the record by Congresswoman Comstock for your response.

Your timely and expeditious responses to these questions are much appreciated. Please respond to these requests at your earliest convenience, but no later than 30 days from the date of this letter.

Should you have any questions, please contact the Subcommittee Staff Director, Dan Mathews, at (202) 225-3014.

Sincerely,

Lou Barletta
Chairman
Subcommittee on Economic Development,
Public Buildings, and Emergency Management

**Questions for the Record for Norman Dong, Commissioner, Public Building Service,
General Services Administration**

Subcommittee on Economic Development, Public Buildings, and Emergency Management

U.S. House Committee on Transportation and Infrastructure

“Saving Taxpayer Dollars by Reducing Federal Office Space Costs”

March 1, 2016

*Questions Submitted by the Subcommittee on Economic Development, Public Buildings, and
Emergency Management on behalf of Representative Barbara Comstock (R-VA-10):*

SUBJECT 1: International Trade Commission building lease:

- 1) What analysis was carried out by GSA Central Office that resulted in GSA reversing its August 2015 approval of the U.S. International Trade Commission’s (ITC) succeeding lease prospectus? What specifically changed between the approval of the succeeding lease prospectus in late August 2015 and the reversal of approval in early October 2015? Can GSA provide any memos or emails that relate to the decision to reverse?
- 2) You stated during the March 1st hearing that GSA wants competition for the ITC just like any other agency. In making this statement, might GSA be overlooking the specific and unique factors associated with the ITC’s lease situation? These include the facts that: (1) they have received no appropriation for the renovations associated with the move; (2) they have received an informal proposal from the current landlord that includes a proposed rent reduction of 20%; (3) they will be able to save rent from this proposal during the current lease term; (4) they are not subject to the “reduce the footprint” requirements; (5) they have unique space requirements related to their need for a courtroom complex; and (6) there will be massive disruption to the agency during an extremely active point in time with regard to U.S. trade policy. How is GSA’s approach in the best interest of the U.S. taxpayer when every analysis to-date of the ITC’s lease situation indicates that the greatest cost savings to the taxpayer will be achieved via a succeeding lease at a reduced rate?
- 3) During the March 1st hearing, you stated a commitment to take into account the disruption costs to the commission in estimating the cost of moving and replicating new space for the ITC. What factors specifically will GSA consider in estimating the disruption cost to the ITC? Will GSA commit to quantifying those costs? Will GSA commit to incorporating the ITC’s estimate of those costs?
- 4) Will GSA commit to including, as a part of the estimate of the cost of moving and replicating the ITC’s space, the lost savings that could be realized by the ITC if GSA had pursued a renegotiation of its current lease as offered by its current landlord?

- 5) In a January 2016 report, GAO found that federal leasing costs increase when tenants finance needed improvements to newly leased space over time (GAO-16-188). In a number of examples, GAO noted that agencies lacked sufficient upfront capital and thus incurred significant interest fees, increasing overall costs of the lease. Given that the ITC received zero appropriated funds for a move and that GSA has no budget authority to fund those costs through its Federal Buildings Fund, what guarantee is in place that the ITC would realize the rent savings that would otherwise be realized under a succeeding lease prospectus?
- 6) Currently, the ITC has mission-critical special space in the form of three courtrooms and a main hearing room. The third courtroom was only recently finished in 2012 at a cost of \$3 million to the U.S. taxpayer. The funds for this new courtroom were specifically appropriated by Congress in order to enable the ITC to expedite the adjudication of its intellectual property cases. Will GSA commit to including this cost in the cost of moving and replicating the ITC's space given that the useful life of the new courtroom extends many years into the future?
- 7) How can the ITC be certain that a new landlord will spend the amount of money necessary to properly build out the space given that the ITC received no appropriation to move and replicate its space? Will GSA commit to including certain specifications or requirements as requested by the ITC in the lease prospectus, the solicitation, and the request for proposal?
- 8) What level of savings does GSA consider necessary to justify moving ITC from its current space? Please take into account, among other costs, the cost of disruption to the agency, the loss in rent savings under ITC's current lease, and the \$3 million recently spent to renovate its current space to add a third courtroom. Is the level of savings that GSA considers necessary to justify moving an agency reflected in a written policy or memorandum? If so, will you provide a copy of such policy or memorandum? Is the level of savings considered necessary by GSA to justify moving an agency the same or similar across agencies? If not, why do they differ? Since it is the ITC that is financially responsible for the rent, will GSA commit to taking into account the ITC's view on whether the potential savings justify the cost of moving?
- 9) The ITC's current lease expires in less than 18 months. If GSA forces ITC to move, it is highly unlikely that a new building could be remodeled to fit the ITC's specifications before the current lease expires. Therefore, does GSA acknowledge that the ITC would likely be forced into a lease holdover or extension if they are forced to move?

SUBJECT 2: Relocation and Consolidation of FBI headquarters:

With regard to the infrastructure surrounding each proposed site:

- 1) What infrastructure changes would need to be made at the Franconia-Springfield site in order to accommodate the FBI headquarters?

- 2) What infrastructure changes would need to be made at the Greenbelt site in order to accommodate the FBI headquarters?
- 3) What infrastructure changes would need to be made at the Landover site in order to accommodate the FBI headquarters?
- 4) What are the strategic benefits associated with relocating the FBI headquarters to the Franconia-Springfield Site?

It is my understanding that GSA has prescribed dollar figures to each potential site which bidders must use as a “baseline” cost when calculating their bid proposals. It is also my understanding that the base number for the Franconia-Springfield site is significantly larger than that of the other two proposed sites.

- 5) What factors were used to arrive at this base figure?
- 6) Is there any flexibility to this base figure associated with the Franconia-Springfield site?
- 7) If the state and local governments offer financial assistance with infrastructure or other needs, can this base figure not be modified?

SUBJECT 3: Social Security Administration headquarters:

In March 2014, the Social Security Administration (SSA) Inspector General (IG) identified a significant amount of unused space both at the SSA headquarters as well as other leased buildings nearby (buildings that were not fully occupied). The IG recommended that SSA look to terminate the costly outlying leases and instead consolidate into a building known as Security West adjacent to the headquarters building in Baltimore.

But rather than heed this advice and pursue a long term lease at Security West—which would have locked in a very reasonable rate for square footage—it is my understanding GSA has issued a prospectus for a different space with a square footage rate that doubles that at Security West.

- 1) Is this a case of the administration adhering to its goal of reducing the footprint?
- 2) Is it acceptable to reduce the footprint even in cases in which doing so will lead to higher costs?



**Committee on Transportation and Infrastructure
U.S. House of Representatives**

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

COMMITTEE RESOLUTION

Mathew M. Sturges, Staff Director

Katherine W. Dedrick, Democratic Staff Director

**CONSTRUCTION
FBI HEADQUARTERS CONSOLIDATION
NATIONAL CAPITAL REGION
PNCR-FBI-NCR17**

Resolved by the Committee on Transportation and Infrastructure of the U.S. House of Representatives, that pursuant to 40 U.S.C. §3307, \$834 million in appropriations are authorized for the site acquisition, design, management and inspection, and construction of a new federally-owned headquarters facility for the Federal Bureau of Investigation of not more than 2.1 million rentable square feet in the National Capital Region for the General Services Administration, for which a prospectus is attached to and included in this resolution.

Provided, the total funds made available through appropriations, including funds transferred to the "Federal Bureau of Investigation, Construction" account, do not exceed \$2.11 billion (excluding the value realized from the exchange of the J. Edgar Hoover building, outfitting, and decommissioning costs).

Provided further, the Administrator considers transportation impacts, including National Capital Planning Commission recommendations on parking and proximity to metro rail.

Provided further, the Administrator considers the total costs to the government for relocations, site preparation, and site acquisition.

Provided further, that such appropriations are authorized only for a project that results in a fully consolidated FBI Headquarters facility.

Provided further, that the Administrator of General Services shall transmit to the Committee on Transportation and Infrastructure of the House of Representative and the Committee on Environment and Public Works of the Senate a report on the construction of a new headquarters for the Federal Bureau of Investigation (FBI). The report transmitted under this provision shall include a summary of the material provisions of the construction and full consolidation of the FBI in a new headquarters facility, including but not limited to, a schedule, the square footage, proposed costs to the Government, and a description of all buildings and infrastructure needed to complete the project.

Provided further, that the Administrator shall not delegate to any other agency the authority granted by this resolution.

Provided further, that the Administrator's authority to make an award of this project expires two years from the date of the adoption of this resolution.

Adopted: December 7, 2016

A handwritten signature in blue ink, appearing to read "Bill Shuster", written over a horizontal line.

Bill Shuster, M.C.
Chairman

**PROSPECTUS – CONSTRUCTION
FBI HEADQUARTERS CONSOLIDATION
NATIONAL CAPITAL REGION**

Prospectus Number: PNCR-FBI-NCR17
Congressional Districts: MD 4,5
VA 8

FY 2017 Project Summary

The General Services Administration (GSA) proposes construction of a new federally owned facility of approximately 2.1 million rentable square feet (RSF)¹ to provide a consolidated Headquarters for the Federal Bureau of Investigation (FBI) in the National Capital Region (NCR). The FBI Headquarters facility will bring together employees from the J. Edgar Hoover Building (JEH) and 13 leased locations across the NCR into a new, modern and secure facility tailored to fully support FBI's national security, intelligence and law enforcement missions. The proposed GSA construction funding in this prospectus will partner with construction funding requested in appropriations to the FBI, FY 2016 enacted appropriations, the value of the JEH exchange and other available FBI resources to support the construction cost of the FBI Headquarters facility.

FY 2017 Committee Approval and Appropriation Requested

(Design, Construction, and Management and Inspection).....\$759,000,000

Overview of Project

As an intelligence-driven and a threat-focused national security organization with both national security and law enforcement responsibilities, the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

The proposed FBI Headquarters facility will consolidate FBI personnel from the JEH and 13 leased locations. The proposed facility will accommodate approximately 11,000 personnel, resulting in an open-plan workspace environment to include state-of-the-art IT infrastructure as required by the FBI's national security mission. The facility will be built to meet ISC Level V security specifications on one of three previously identified sites. Initial programming provides 6,697 to 8,155 structured and unstructured parking spaces² for official vehicles, employees, and visitors.

At the time of project initiation, the FBI was housed in 21 locations throughout the NCR, including JEH, occupying an aggregate total of 3,029,709 rentable square feet. Over the

¹ This prospectus references an estimated total rentable square feet. The total rentable square footage will vary depending upon the final rentable to usable factor which will be determined by the winning bid, design and selected site.

² The actual amount of parking required will be dependent upon final site selection and the availability of alternate means of transportation.

**PROSPECTUS – CONSTRUCTION
FBI HEADQUARTERS CONSOLIDATION
NATIONAL CAPITAL REGION**

Prospectus Number: PNCR-FBI-NCR17
Congressional Districts: MD 4,5
VA 8

intervening years, FBI has taken a number of actions resulting in a decrease in the agency's footprint. Today, FBI Headquarters functions in the NCR are housed in 14 locations, totaling 2,930,552 rentable square feet. Staff in each of these 14 locations will be consolidated into the new FBI Headquarters facility. The precise RSF for the new FBI Headquarters facility will vary based on the final R/U factor which is dependent upon the winning bid, design and selected site.

Location and Site Area

The project includes conveying title to JEH to the winning bidder in exchange for a newly constructed FBI Headquarters facility at one of the three previously identified potential sites in Greenbelt, MD, Landover, MD, and Springfield, VA.

Greenbelt..... 61 acres
Greenbelt – Comprised of approximately 61 acres of land owned by the State of Maryland and the Washington Metropolitan Area Transit Authority (WMATA), and controlled by GSA pursuant to a purchase option agreement. Located at the Greenbelt Metrorail Station, in Prince George's County, Maryland.

Landover 80 acres
Landover – Comprised of approximately 80 acres, privately owned, and controlled by GSA pursuant to a purchase option agreement between GSA and the current site owner. Located at the site of the former Landover Mall, in Prince George's County, Maryland.

Springfield..... 58 acres
Springfield - Comprised of approximately 58 acres of federally owned land under the custody and control of GSA. Located at the current site of the GSA Franconia Warehouse Complex in Fairfax County, Virginia.

Building Area

The proposed transaction allows the bidders to submit proposals to construct the FBI Headquarters facility on one of the three sites described above. Bidders have the opportunity to submit proposals on one, two or all three of the identified potential sites.

Building (excluding parking)..... 2,100,000 RSF

Bidders are required to accommodate parking consistent with the number of spaces required for each location: 6,697 spaces for Greenbelt; 8,155 spaces for Landover; 7,039

**PROSPECTUS – CONSTRUCTION
FBI HEADQUARTERS CONSOLIDATION
NATIONAL CAPITAL REGION**

Prospectus Number: PNCR-FBI-NCRI7
Congressional Districts: MD 4,5
VA 8

spaces for Springfield, each inclusive of 425 official vehicles (including Bureau Cars and FBI police). Distribution between structured and unstructured parking will be dependent upon the site and the proposal made by the bidder.

Project Budget

The costs of the consolidated FBI Headquarters facility will be supported by: (1) FY 2016 enacted funds from the Omnibus Consolidated Appropriations Act, which included \$180 million in FBI construction funding, \$135 million in resources made available from the FBI's prior year balances, and \$75 million in GSA FBF construction funding; (2) the value realized from the exchange of the JEH; (3) the President's Fiscal Year 2017 budget proposal of \$759 million in construction funding within the GSA FBF; and (4) the President's Fiscal Year 2017 budget proposal of \$646 million in the FBI's Construction account. Combined, these funds should ensure that GSA is in a position to award the project on schedule in FY 2017, and support the design and construction of the full consolidation. It is anticipated that outfitting and transition costs will be addressed by the FBI in future years.

Schedule

	Start	End*
GSA Construction Management/Oversight Activities	FY 2016	FY 2022
Design and Construction	FY 2017	FY 2022

*(Identified end dates for both management and oversight, and design and construction are estimates. Actual schedules will be established following award with the winning bidder during design development.)

Tenant Agencies

Federal Bureau of Investigation

Justification

The FBI is in urgent need of a consolidated Headquarters facility to support information sharing, collaboration, and integration of strategic priorities. Currently, FBI Headquarters elements are dispersed over 14 locations in the greater Washington, DC area. This dispersion and fragmentation has created significant challenges to effective command and control and to facilitating organizational change. Dispersion diverts time and resources, hampers coordination, decreases flexibility, and impedes the FBI's ability to rapidly respond to ever changing, asymmetric threats. The FBI needs a consolidated Headquarters facility and operations center to support information sharing, collaboration and integration of strategic priorities. By consolidating into a single location, FBI will

**PROSPECTUS – CONSTRUCTION
FBI HEADQUARTERS CONSOLIDATION
NATIONAL CAPITAL REGION**

Prospectus Number: PNCR-FBI-NCR17
Congressional Districts: MD 4,5
VA 8

realize significant mission synergies, and greatly increase workforce and mission security compared to the varying risk scenarios existing throughout the current facilities.

The FBI has occupied JEH since 1974. The approximately 1.8 million rentable square foot (2.4 million gross square foot) JEH sits on 6.7 acres of land fronting Pennsylvania Avenue and is a prime location for office, retail, and residential uses. The building was designed at a time when FBI operated differently, and it cannot be redeveloped to provide the necessary space to consolidate the FBI Headquarters components or to meet the agency's physical security and current and projected operational requirements. Furthermore the IT infrastructure in JEH has reached capacity and cannot be expanded further. These challenges can best be addressed through consolidation and by providing a flexible infrastructure capable of supporting multiple IT systems. The JEH was not designed to support today's FBI mission that includes an increased emphasis on national security.

JEH and virtually all of the 13 offsite leased facilities do not meet the applicable Interagency Security Committee (ISC) Standards. Senate Report 110-397 – Departments of Commerce and Justice, Science, and Related Agencies Appropriations Bill, 2009, concluded that JEH does not meet the ISC physical security criteria. As the central facility for the management of intelligence and national security programs, the FBI Headquarters facility must have high reliability and survivability of utilities and infrastructure.

Due to the critical need for continuous operations of the FBI, the consolidated FBI Headquarters must be resilient to safeguard the mission it houses and remain operational and capable in the event of local or regional emergency. The facility must provide the FBI the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions. In order to achieve resilience, the program includes utility and building systems redundancy, back-up power generation and water storage requirements, and energy and water efficiency targets. Requirements for utility redundancy include dual feeds for communications, electric service, potable water, and natural gas. Where appropriate, delivery of building services must also be redundant to ensure continued operability in the event of a disruption internal to the facility.

Summary of Energy Compliance

The consolidated FBI Headquarters facility will be designed to attain a Gold rating in the Leadership in Energy and Environmental Design (LEED) Building Design and Construction (BD+C) rating system, as required by GSA policy for new Federal

**PROSPECTUS – CONSTRUCTION
FBI HEADQUARTERS CONSOLIDATION
NATIONAL CAPITAL REGION**

Prospectus Number: PNCR-FBI-NCR17
Congressional Districts: MD 4,5
VA 8

facilities. Furthermore, it will be LEED Operations and Maintenance (O+M) “ready” to ensure that the building systems are operated and maintained efficiently over the long term, protecting the government’s investment.

Energy and Resources – Design, construction, and ongoing operation of the facility will minimize the impact on the environment and the utilization of energy and other scarce and non-renewable resources. The project will consider operational requirements, and focus on strategies that support energy surety goals, incorporating principles of energy source diversity, onsite renewable energy, energy storage, net-zero energy readiness, and micro-grids, as appropriate, informed by mission goals and life-cycle cost analyses.

Sustainability – Design and construction of the facility will achieve a minimum of LEED Gold rating in the BD+C v4 rating system. The new facility will comply with all applicable federal sustainability requirements. It will also consider operational requirements, and incorporate principles of passive design, onsite management of storm-water and waste, resource efficiency, human health and well-being, and life cycle costing.

Reliability and Resilience – The facility will be designed to have high reliability and survivability of utilities and infrastructure. It will include efficient, state-of-the-art HVAC, lighting, power, security, and telecommunications systems and equipment that require minimal maintenance and are designed with backup capabilities to ensure minimal loss of service or downtime. Design of the site and buildings will include principles of energy and water surety, and resistance and resilience to climate change. Incremental climate change impacts, extreme weather conditions, and/or other extreme events, will result in minimal disruption to the mission of the FBI Headquarters complex and the safety of its occupants. The building enclosure systems and critical building systems will be designed to optimize performance and resilience in response to potential extreme events and conditions.

Prior Appropriations

Prior Appropriations			
Public Law	Fiscal Year	Amount	Purpose
114-113	2016	\$75,000,000	Construction Management and oversight activities and other project support costs
Appropriations to Date		\$75,000,000	

**PROSPECTUS – CONSTRUCTION
FBI HEADQUARTERS CONSOLIDATION
NATIONAL CAPITAL REGION**

Prospectus Number: PNCR-FBI-NCR17
Congressional Districts: MD 4,5
VA 8

Prior Committee Approvals

None

Alternatives Considered

The proposed state-of-the-art FBI Headquarters facility is a unique asset, built to the Government's specifications in the form of a detailed Program of Requirements. The proposed facility will meet the long term needs of the FBI. GSA analyzed the modernization and redevelopment of JEH, but in addition to being cost prohibitive, the current facility as sited is not capable of meeting the square footage, security setback, or operational requirements of the FBI. A leased alternative is not cost-effective given FBI's 46 year history in the current location and the stated 50+ year requirement for the proposed facility. A leased alternative is not considered to be cost effective and the 30 year present value of such alternative was not analyzed.

Recommendation

CONSTRUCTION

**PROSPECTUS – CONSTRUCTION
FBI HEADQUARTERS CONSOLIDATION
NATIONAL CAPITAL REGION**

Prospectus Number: PNCR-FBI-NCR17
Congressional Districts: MD 4,5
VA 8

Certification of Need

The proposed project is the best solution to meet a validated Government need.

Submitted at Washington, DC, on February 8, 2016

Recommended: 

Commissioner, Public Buildings Service

Approved: 

Administrator, General Services Administration



Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

COMMITTEE RESOLUTION

Mathew M. Sturges, Staff Director

NEW U.S. COURTHOUSE
ANNISTON, AL
PAL-CTC-AN16

Katherine W. Dedrick, Democratic Staff Director

Resolved by the Committee on Transportation and Infrastructure of the U.S. House of Representatives, that pursuant to 40 U.S.C. §3307, appropriations are authorized for the site acquisition, design and construction of a new U.S. Courthouse of approximately 63,000 gross square feet, including approximately 13 parking spaces, in Anniston, Alabama at an additional site and design cost of \$2,414,000, a total estimated construction cost of \$32,527,000, and total management and inspection cost of \$3,234,000 for a total estimated project cost, including prior authorizations, of \$42,575,000, for which a prospectus is attached to and included in this resolution. This resolution amends prior authorizations of July 24, 2002 and July 23, 2003.

Provided, that the Administrator of General Services shall ensure that construction of the new courthouse complies, at a minimum, with courtroom sharing requirements adopted by the Judicial Conference of the United States.

Provided further, that the Administrator of General Services shall ensure that the construction of the new courthouse contains no more than two courtrooms, including one for Senior District Judges and one for Bankruptcy Judges.

Provided further, that the design of the new courthouse shall not deviate from the U.S. Courts Design Guide.

Adopted: December 7, 2016

Bill Shuster, M.C.
Chairman

**PROSPECTUS
NEW U.S. COURTHOUSE
ANNISTON, AL**

Prospectus Number: PAL-CTC-AN16
Congressional District: 03

FY 2016 Project Summary

The General Services Administration (GSA) proposes the acquisition of a site, and the design and construction of a new U.S. Courthouse of approximately 63,000 gross square feet (gsf), including 13 inside parking spaces in Anniston, AL. GSA will construct the courthouse to meet the 10-year space needs of the court and court-related agencies and the site will accommodate the anticipated 30-year needs of the court. The Judiciary's Courthouse Project Priorities list (approved by the Judicial Conference of the United States on September 17, 2015) includes a courthouse project in Anniston, AL.

FY 2016 House and Senate Committee Approval Requested

(Additional Site and Design, Construction, Management & Inspection)\$38,175,000

FY 2016 Funding Requested (as outlined in the FY 2016 Spend Plan)

(Additional Site and Design, Construction, Management & Inspection)\$38,175,000

Overview of Project

The courts and related agencies are currently located in the Federal Building-Courthouse (FB-CT) as well as one leased location in Anniston. The FB-CT, built in 1906, is listed in the National Register of Historic Places. The new courthouse will provide two courtrooms and three chambers consistent with the application of courtroom sharing policies and limitation on the provision of space for projected judgeships. The site for the new courthouse will be in the central business area of Anniston.

Site Information

To Be Acquired Approximately 3 acres

Building Area¹

Gross square feet (excluding inside parking)57,000
Gross square feet (including inside parking)63,000
Inside parking spaces 13

¹ Square footages and number of parking spaces are approximate. The actual project may contain a variance in gross square footage from that listed in this prospectus.

**PROSPECTUS
NEW U.S. COURTHOUSE
ANNISTON, AL**

Prospectus Number: PAL-CTC-AN16
Congressional District: 03

Estimated Project Budget

Site Cost (FY 2004)	\$2,500,000
Estimated Additional Site	\$554,000
Design (FY 2004)	\$1,900,000
Estimated Additional Design	\$1,860,000
Estimated Construction Cost (ECC) (\$516/gsf, including inside parking)	\$32,527,000
Estimated Management and Inspection (M&I)	\$3,234,000
Estimated Total Project Cost (ETPC)*	\$42,575,000²

*Tenant agencies may fund an additional amount for alterations above the standard normally provided by GSA.

Schedule

	Start	End
Design & Construction	FY 2016	FY 2021

Tenant Agencies

U.S. District Court, U.S. Bankruptcy Court, U.S. Probation Office, U. S. Department of Justice - Marshals Service, trial preparation space for the U.S. Department of Justice - Office of the U.S. Attorney, and GSA.

Justification

The existing FB-CT, constructed in 1906 and expanded in 1935, does not meet the U.S. Courts Design Guide standards, does not provide for future expansion, and lacks adequate security. There is no separate circulation for judicial officers and prisoners, and no secure elevators in the building. Further, there are no courtroom holding cells, central cellblock, prisoner sallyport, and no secured parking available to the courts. The new courthouse will provide separate circulation for the public, judges, and prisoners, thereby improving security, as well as the efficiency of court operations. Relocation of agencies from leased space to the new courthouse will result in savings of approximately \$195,000 in future annual lease payments to the private sector.

Due to changes in program since previous project approval, courtroom sharing, and exclusion of projected new judgeships, the proposed project has decreased in size and scope (from the previously approved 65,482 gsf).

² GSA requests approval for a total project cost. As noted in the estimated project budget above, GSA identified sub-totals comprising the estimated project budget are intended to provide a breakdown in support of the ETPC. The actual total cost to perform the entire project may differ from what is represented in this prospectus by the various subcomponents.

**PROSPECTUS
NEW U.S. COURTHOUSE
ANNISTON, AL**

Prospectus Number: PAL-CTC-AN16
Congressional District: 03

Space Requirements of the U.S. Courts

	Current		Proposed	
	Courtrooms	Judges	Courtrooms	Judges
District				
- Active	1	1	0	0
- Senior	0	0	1	1
- Visiting	0	0		1
Bankruptcy	1	1	1	1
Total:	2	2	2	3

Summary of Energy Compliance

This project will be designed to conform to requirements of the Facilities Standards for the Public Buildings Service and will implement strategies to meet the Guiding Principles for High Performance and Sustainable Buildings. GSA encourages design opportunities to increase energy and water efficiency above the minimum performance criteria.

Future of Existing Federal Building³

The Federal tenancy in Anniston does not support the need for two courthouses; therefore, GSA will explore alternatives associated with the disposal of the existing courthouse. Some of these alternatives include donation or exchange.

³ This section is included to address recommendations in the following GAO Report: Federal Courthouses: Better Planning Needed Regarding Reuse of Old Courthouses (GAO-14-48).

**PROSPECTUS
NEW U.S. COURTHOUSE
ANNISTON, AL**

Prospectus Number: PAL-CTC-AN16
Congressional District: 03

Prior Appropriations

Prior Appropriations			
Public Law	Fiscal Year	Amount	Proposed Project
108-199	2004	\$4,400,000	Site and Design
114-113*	2016	\$38,175,000	Additional Site & Design, ECC & M&I
Appropriations to Date		\$42,575,000	

*Public Law 114-113 funded \$947,760,000 for new construction projects of the Federal Judiciary as prioritized in the Federal Judiciary Courthouse Project Priorities list, of which Anniston is included. GSA's Spend Plan describes each project to be undertaken with this funding. The FY 2016 need for Anniston is \$38,175,000.

Prior Committee Approvals

Prior Committee Approvals			
Committee	Date	Amount	Proposed Project
House T&I	7/24/2002	\$3,090,000	Site and Design for 65,482 gsf; 20 inside parking spaces
Senate EPW	9/26/2002	\$3,090,000	Site and Design for 65,482 gsf; 20 inside parking spaces
House T&I	7/23/2003	\$1,291,000	Additional Site and Design for 65,482 gsf; 20 inside parking spaces
Senate EPW	6/23/2004	\$1,291,000	Additional Site and Design for 65,482 gsf; 20 inside parking spaces
House Approvals to Date		\$4,381,000	
Senate Approvals to Date		\$4,381,000	

**PROSPECTUS
NEW U.S. COURTHOUSE
ANNISTON, AL**

Prospectus Number: PAL-CTC-AN16
Congressional District: 03

Certification of Need

The proposed project is the best solution to meet a validated Government need.

Submitted at Washington, DC, on

JUN 16 20

Recommended:



Commissioner, Public Buildings Service

Approved:



Administrator, General Services Administration

(b) (7) (F)

Provided further, that the General Services Administration shall not delegate to any other agency the authority granted by this resolution.

Adopted: December 7, 2016

A handwritten signature in blue ink, appearing to read "Bill Shuster", is written over a horizontal line.

Bill Shuster, M.C.
Chairman

**PROSPECTUS – LEASE
DEPARTMENT OF HOMELAND SECURITY
CUSTOMS AND BORDER PROTECTION
OFFICE OF INFORMATION TECHNOLOGY
NORTHERN, VA**

Prospectus Number: PVA-01-WA17
Congressional Districts: 8, 10, 11

Executive Summary

The General Services Administration (GSA) proposes a lease for approximately 562,000 rentable square feet (RSF) of space for the Department of Homeland Security (DHS), Customs and Border Protection (CBP), Office of Information Technology (OIT), currently located in leased space in 11 separate buildings dispersed across six locations including six buildings in the VA-95 complex located at Boston Boulevard and Fullerton Road in Springfield, VA. Other locations are 1801 N. Beauregard St., Alexandria, VA; 6350 Walker Lane, Springfield, VA; 7799 Leesburg Pike, Falls Church, VA; 13990 Park East Circle, Chantilly, VA; and 5971 Kingstowne Village Parkway, Alexandria, VA.

The lease will enable DHS/CBP/OIT to provide continued housing as well as more modern, streamlined, and efficient operations. It will significantly improve space utilization, as the office utilization rate will be improved from 113 to 64 usable square feet (USF) per person, and the overall utilization rate from 184 to 124 USF per person, reducing the DHS/CBP/OIT footprint for this occupancy by approximately 67,680 RSF.

Description

Occupant:	Customs and Border Protection
Current Rentable Square Feet (RSF)	629,680 (Current RSF/USF = 1.08)
Proposed Maximum RSF ¹ :	562,000 (Proposed RSF/USF = 1.20)
Expansion/Reduction RSF:	67,680 (Reduction)
Current Usable Square Feet/Person:	184
Proposed Usable Square Feet/Person:	124
Proposed Maximum Leasing Authority:	15 years
Expiration Dates of Current Lease(s):	09/30/19, 08/01/20, 12/07/20, 12/31/20, 5/31/21, 08/10/21
Delineated Area:	Northern Virginia
Number of Official Parking Spaces ² :	4
Scoring:	Operating Lease
Maximum Proposed Rental Rate ³ :	\$39.00/RSF

¹ The RSF/USF at the current location is approximately 1.08; however, to maximize competition a RSF/USF ratio of 1.20 is used for the proposed maximum RSF as indicated in the housing plan.

² OIT security requirements may necessitate control of the parking at the leased location. This may be accomplished as a lessor-furnished service, as a separate operating agreement with the lessor, or as part of the Government's leasehold interest in the building.

**PROSPECTUS – LEASE
DEPARTMENT OF HOMELAND SECURITY
CUSTOMS AND BORDER PROTECTION
OFFICE OF INFORMATION TECHNOLOGY
NORTHERN, VA**

Prospectus Number: PVA-01-WA17
Congressional Districts: 8, 10, 11

Proposed Total Annual Cost ⁴ :	\$21,918,000
Current Total Annual Cost:	\$17,079,000 (Leases effective: 10/01/94, 12/08/00, 01/17/02, 07/15/02, 08/02/05, 11/14/07, 11/21/08, 02/02/09, 06/01/11, and 08/11/11)

Background

OIT is responsible for implementation and support of information technology, research and development functions, and automation and technological strategies for meeting mission-related needs. OIT is responsible for automated information systems, management of the research and development functions, and all forensic and laboratory support of CBP. OIT personnel manage all computer and related resources and establish requirements for computer interfaces between CBP and various trade groups and Government agencies. OIT is responsible for managing all aspects of tactical communications, including the 24/7 operations of the National Law Enforcement Communications Center and Continuity of Operations Planning.

Justification

OIT's mission is to be responsible for all aspects of technology support across all mission areas within CBP. This CBP component designs, develops, programs, tests, implements, trains, and maintains the agency's automated systems. OIT is responsible for managing CBP computer facilities, including all the hardware, software, data, video and voice communications, and related financial resources. OIT develops and maintains the Enterprise Information System Architecture and administers the operational aspects of the CBP Computer Security Program. OIT also represents CBP on matters related to automated import, export, and interagency processing and systems development.

³ These estimates are for fiscal year 2017 and may be escalated by 1.95 percent annually to the effective date of the lease to account for inflation. The proposed rental rates are fully serviced including all operating expenses whether paid by the lessor or directly by the Government. GSA will conduct the procurement using prevailing market rental rates as a benchmark for the evaluation of competitive offers and as the basis for negotiating with offerors to ensure that lease award is made in the best interest of the Government.

⁴ New leases may contain an escalation clause to provide for annual changes in real estate taxes and operating costs.

**PROSPECTUS – LEASE
DEPARTMENT OF HOMELAND SECURITY
CUSTOMS AND BORDER PROTECTION
OFFICE OF INFORMATION TECHNOLOGY
NORTHERN, VA**

Prospectus Number: PVA-01-WA17
Congressional Districts: 8, 10, 11

The current leases are for space in 11 separate buildings in Northern Virginia and expire between September 30, 2019 and August 10, 2021. OIT requires continued housing to carry out its operational mission and functions. The total space requested will reduce the OIT footprint by 67,680 RSF or more than 10 percent of the 629,680 RSF currently occupied. In the absence of this reduction, the status quo cost of continued occupancy at the proposed market rental rate would be at least \$24.6 million per year.

Acquisition Strategy

In order to maximize the flexibility and competition in acquiring space to house the DHS/CBP/OIT elements, GSA may issue a single, multiple award solicitation that will allow offerors to provide blocks of space able to meet requirements in whole or in part. All offers must provide space consistent with the delineated area defined by this prospectus.

Summary of Energy Compliance

GSA will incorporate energy efficiency requirements into the Request for Lease Proposals and other documents related to the procurement of space based on the approved prospectus. GSA encourages offerors to exceed minimum requirements set forth in the procurement and to achieve an Energy Star performance rating of 75 or higher.

Resolutions of Approval

Resolutions adopted by the House Committee on Transportation and Infrastructure and the Senate Committee on Environment and Public Works approving this prospectus will constitute approval to make appropriations to lease space in a facility that will yield the required rentable area.

Interim Leasing

GSA will execute such interim leasing actions as are necessary to ensure continued housing of the tenant agency prior to the effective date of the new lease. It is in the best interest of the Government to avert the financial risk of holdover tenancy.

**PROSPECTUS - LEASE
DEPARTMENT OF HOMELAND SECURITY
CUSTOMS AND BORDER PROTECTION
OFFICE OF INFORMATION TECHNOLOGY
NORTHERN, VA**

Prospectus Number: PVA-01-WA17
Congressional Districts: 8, 10, 11

Certification of Need

The proposed project is the best solution to meet a validated Government need.

Submitted at Washington, DC, on September 15, 2016

Recommended: 

Commissioner, Public Buildings Service

Approved: 

Administrator, General Services Administration

(b) (7) (F)



**Committee on Transportation and Infrastructure
U.S. House of Representatives**

**Bill Shuster
Chairman**

Washington, DC 20515

**Peter A. DeFazio
Ranking Member**

COMMITTEE RESOLUTION

Mathew M. Sturges, Staff Director

Katherine W. Dedrick, Democratic Staff Director

**LEASE
FOOD & DRUG ADMINISTRATION
ATLANTA, GA
PGA-01-AT17**

Resolved by the Committee on Transportation and Infrastructure of the U.S. House of Representatives, that pursuant to 40 U.S.C. §3307, appropriations are authorized for a lease of up to 162,000 rentable square feet of space, including 27 official parking spaces, for the Food and Drug Administration currently located at the FDA Atlanta complex consisting of three leased buildings; Crawford Building, Annex I and Annex II, and an additional lease location in College Park, Georgia at a proposed total annual cost of \$5,994,000 for a lease term of up to 20 years, a prospectus for which is attached to and included in this resolution.

Approval of this prospectus constitutes authority to execute an interim lease for all tenants, if necessary, prior to the execution of the new lease.

Provided that, the Administrator of General Services and tenant agencies agree to apply an overall utilization rate of 322 square feet or less per person, except that, if the Administrator determines that the overall utilization rate cannot be achieved, the Administrator shall provide an explanatory statement to the Committee on Transportation and Infrastructure of the House of Representatives prior to exercising any lease authority provided in this resolution.

Provided that, except for interim leases as described above, the Administrator may not enter into any leases that are below prospectus level for the purposes of meeting any of the requirements, or portions thereof, included in the prospectus that would result in an overall utilization rate of 322 square feet or higher per person.

Provided that, to the maximum extent practicable, the Administrator shall include in the lease contract(s) a purchase option.

Provided further, that the Administrator shall require that the delineated area of the procurement is identical to the delineated area included in the prospectus, except that, if the Administrator determines that the delineated area of the procurement should not be identical to the delineated area included in the prospectus, the Administrator shall provide an explanatory statement to the Committee on Transportation and Infrastructure of the House of Representatives prior to exercising any lease authority provided in this resolution.

Provided further, that the General Services Administration shall not delegate to any other agency the authority granted by this resolution.

Adopted: December 7, 2016

A handwritten signature in blue ink, appearing to read "Bill Shuster", with a stylized flourish at the end.

Bill Shuster, M.C.
Chairman

**PROSPECTUS - LEASE
FOOD & DRUG ADMINISTRATION
ATLANTA, GA**

Prospectus Number: PGA-01-AT17

Congressional District: 5

Executive Summary

The General Services Administration (GSA) proposes a lease of approximately 162,000 rentable square feet (RSF) of space for the Food and Drug Administration (FDA), currently housed at the FDA Atlanta complex consisting of three leased buildings; The Crawford Building, Annex I and Annex II, and an additional lease location in College Park, Georgia, at the Gateway Center Building One.

The proposed lease will provide continued housing for FDA and will improve the office utilization rate from 176 to 103 usable square feet (USF) per person.

Description

Occupant:	Food and Drug Administration
Current Rentable Square Feet (RSF)	134,491 (Current RSF/USF = 1.15)
Estimated Maximum RSF:	162,000 (Proposed RSF/USF = 1.15)
Expansion/Reduction RSF:	27,509 (expansion)
Current Usable Square Feet/Person:	292
Estimated Usable Square Feet/Person:	322
Proposed Maximum Lease Term:	20 Years
Expiration Dates of Current Leases:	11/24/2017, 12/30/2017, and 7/31/2022
Delineated Area:	Atlanta Midtown Business District
Number of Official Parking Spaces:	27 secured
Scoring:	Operating lease
Estimated Rental Rate ¹ :	37.00/RSF
Estimated Total Annual Cost ² :	\$5,994,000
Current Total Annual Cost:	\$5,863,625 (Leases effective 11/25/2005, 12/31/1997, 8/1/2012)

¹ This estimate is for Fiscal Year 2019 and may be escalated by 2.0 percent annually to the effective date of the lease to account for inflation. The proposed rental rate is fully serviced including all operating expenses whether paid by the lessor or directly by the Government. GSA will conduct the procurement using prevailing market rental rates as a benchmark for the evaluation of competitive offers and as a basis for negotiating with offerors to ensure that lease award is made in the best interest of the government.

² New leases may contain an escalation clause to provide for annual changes in real estate taxes and operating costs.

**PROSPECTUS – LEASE
FOOD & DRUG ADMINISTRATION
ATLANTA, GA**

Prospectus Number: PGA-01-AT17
Congressional District: 5

Justification

The current leases are unable to provide the FDA Southeast Regional Office, Atlanta District Office, and Southeast Regional Laboratories (SRL) with the necessary office and special space to efficiently carry out its mission. The new lease will provide a more modern and streamlined office layout and improve office utilization from 176 square feet per person to 103 square feet per person.

SRL testing includes foods, ceramics, meats, cosmetics, drugs, and other products falling under the purview of the FDA. In addition, the SRL has specialized capabilities and is home to the Atlanta Center for Nutrient Analysis, which is the servicing laboratory to all FDA districts for nutrient analysis on domestic and imported foods that bear nutrition labeling. The size of the existing SRL causes the FDA to constantly retro-fit the aging space, leading to higher maintenance costs. A modern laboratory is needed to properly carry out its mission.

Acquisition Strategy

In order to maximize the flexibility in acquiring space to house the FDA elements, GSA may issue a single, multiple award solicitation that will allow offerors to provide blocks of space able to meet requirements in whole or in part. All offers must provide space consistent with the delineated area defined by this prospectus.

Summary of Energy Compliance

GSA will incorporate energy efficiency requirements into the Request for Lease Proposals and other documents related to the procurement of space based on the approved prospectus. GSA encourages offerors to exceed minimum requirements set forth in the procurement and to achieve an Energy Star performance rating of 75 or higher.

Resolutions of Approval

Resolutions adopted by the House Committee on Transportation and Infrastructure and the Senate Committee on Environment and Public Works approving this prospectus will constitute approval to make appropriations to lease space in a facility that will yield the required rentable area.

PROSPECTUS - LEASE
FOOD & DRUG ADMINISTRATION
ATLANTA, GA

Prospectus Number: PGA-01-AT17
Congressional District: 5

Interim Leasing

GSA will execute such interim leasing actions as are necessary to ensure continued housing of the tenant agency prior to the effective date of the new lease. It is in the best interest of the Government to avert the financial risk of holdover tenancy.

Certification of Need

The proposed lease is the best solution to meet a validated Government need.

Submitted at Washington, DC, on SEP 13 2016

Recommended: 

Commissioner, Public Buildings Service

Approved: 

Administrator, General Services Administration

(b) (7) (F)



**Committee on Transportation and Infrastructure
U.S. House of Representatives**

**Bill Shuster
Chairman**

Washington, DC 20515

**Peter A. DeFazio
Ranking Member**

AMENDED COMMITTEE RESOLUTION

Mathew M. Sturges, Staff Director

Katherine W. Dedrick, Democratic Staff Director

**LEASE
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
JACKSON AND CLAY COUNTIES, MISSOURI, AND JOHNSON COUNTY, KANSAS
PMO-01-LS17**

Resolved by the Committee on Transportation and Infrastructure of the U.S. House of Representatives, that pursuant to 40 U.S.C. §3307, appropriations are authorized for a lease of up to 806,794 rentable square feet of space, including 142 official parking spaces, for the National Archives and Records Administration, Federal Records Center currently located at 200 NW Space Center in Lee's Summit, Missouri at a proposed total annual cost of \$5,647,558 for a lease term of up to 20 years, a prospectus for which is attached to and included in this resolution. This resolution amends the resolution adopted by the Committee on Transportation and Infrastructure on September 14, 2016.

Approval of this prospectus constitutes authority to execute an interim lease for all tenants, if necessary, prior to the execution of the new lease.

Provided that, the Administrator of General Services and tenant agencies agree to apply an office utilization rate of 129 square feet or less per person, except that, if the Administrator determines that the office utilization rate cannot be achieved, the Administrator shall provide an explanatory statement to the Committee on Transportation and Infrastructure of the House of Representatives prior to exercising any lease authority provided in this resolution.

Provided that, except for interim leases as described above, the Administrator may not enter into any leases that are below prospectus level for the purposes of meeting any of the requirements, or portions thereof, included in the prospectus that would result in an office utilization rate of 129 square feet or higher per person.

Provided that, to the maximum extent practicable, the Administrator shall include in the lease contract(s) a purchase option.

Provided further, that the Administrator shall require that the delineated area of the procurement is identical to the delineated area included in the prospectus, except that, if the Administrator determines that the delineated area of the procurement should not be identical to the delineated area included in the prospectus, the Administrator shall provide an explanatory statement to the Committee on Transportation and Infrastructure of the House of Representatives prior to exercising any lease authority provided in this resolution.

Provided further, that the General Services Administration shall not delegate to any other agency the authority granted by this resolution.

Adopted: **December 7, 2016**

A handwritten signature in blue ink, appearing to read "Bill Shuster", with a stylized flourish at the end.

Bill Shuster, M.C.
Chairman

**PROSPECTUS – LEASE
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
JACKSON AND CLAY COUNTIES, MISSOURI, AND JOHNSON
COUNTY, KANSAS**

Prospectus Number: PMO-01-LS17
Congressional District: MO 05, 06, KS 03

Executive Summary

The General Services Administration (GSA) proposes a lease of approximately 806,794 rentable square feet (RSF) for the National Archives and Records Administration – Federal Records Center (NARA-FRC), currently located at 200 NW Space Center, Lee's Summit, MO.

The lease will provide continued housing for NARA-FRC, will maintain its current office utilization rate of 129 usable square feet (USF) per person, and allow for continued temporary and permanent record storage capabilities for Federal agencies.

Description

Occupant:	National Archives and Records Administration
Current Rentable Square Feet (RSF)	806,794 (Current RSF/USF = 1.00)
Estimated Maximum RSF:	806,794 (Proposed RSF/USF = 1.00)
Expansion/Reduction RSF:	None
Current Usable Square Feet/Person:	129
Estimated Usable Square Feet/Person:	129
Proposed Maximum Lease Term:	20 Years
Expiration Dates of Current Leases:	8/14/2017
Delineated Area:	Jackson and Clay Counties, Missouri, and Johnson County, Kansas
Number of Official Parking Spaces:	142
Scoring:	Operating lease
Estimated Rental Rate ¹ :	\$7.00 / RSF

¹This estimate is for fiscal year 2017 and may be escalated by 2.0 percent annually to the effective date of the lease to account for inflation. The proposed rental rate is fully serviced including all operating expenses whether paid by the lessor or directly by the Government. GSA will conduct the procurement using prevailing market rental rates as a benchmark for the evaluation of competitive offers and as a basis for negotiating with offerors to ensure that lease award is made in the best interest of the Government.

**PROSPECTUS – LEASE
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
JACKSON AND CLAY COUNTIES, MISSOURI, AND JOHNSON
COUNTY, KANSAS**

Prospectus Number: PMO-01-LS17
Congressional District: MO 05, 06, KS 03

Estimated Total Annual Cost ² :	\$5,647,558
Current Total Annual Cost:	\$3,211,969 (Lease effective 8/15/1997)

Acquisition Strategy

The NARA-FRC is currently located in subterranean space. In order to maximize competition, GSA will consider aboveground and subterranean space for this procurement and will relocate the agency if economically advantageous to the Federal Government.

Justification

NARA-FRC is one of 18 Federal Records Centers across the nation used by Federal agencies for records-related services. The FRCs work together to provide temporary and permanent record storage services. The facility storage services are full at this location and any new incoming client boxes are accommodated by moving existing records to other Federal Records Centers or by the disposal of eligible records. The current location provides storage conditions that meet permanent or archival requirements, which accounts for 57 percent of permanent record storage.

NARA-FRC requires space to accommodate the movement, processing, and retrieving of large quantities of client record boxes into its computer systems, along with the ability to store client records in an environment that meets regulations for Federal Records Storage (36 CFR 1234). The movement of client record boxes is accommodated using eight-foot carts, which require ample circulation space for maneuvering. Although Federal agencies are attempting to convert to electronic storage, the demand for paper record storage still remains and since 2000 has grown by 2.38 percent per year.

²New leases may contain an escalation clause to provide for annual changes in real estate taxes and operating costs.

**PROSPECTUS – LEASE
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
JACKSON AND CLAY COUNTIES, MISSOURI, AND JOHNSON
COUNTY, KANSAS**

Prospectus Number: PMO-01-LS17
Congressional District: MO 05, 06, KS 03

Summary of Energy Compliance

GSA will incorporate energy efficiency requirements into the Request for Lease Proposals and other documents related to the procurement of space based on the approved prospectus. GSA encourages offerors to exceed minimum requirements set forth in the procurement and to achieve an Energy Star performance rating of 75 or higher.

Resolutions of Approval

Resolutions adopted by the House Committee on Transportation and Infrastructure and the Senate Committee on Environment and Public Works approving this prospectus will constitute approval to make appropriations to lease space in a facility that will yield the required rentable area.

Interim Leasing

GSA will execute such interim leasing actions as are necessary to ensure continued housing of the tenant agency prior to the effective date of the new lease. It is in the best interest of the Government to avert the financial risk of holdover tenancy.

GSA

PBS

**PROSPECTUS – LEASE
NATIONAL ARCHIVES AND RECORDS ADMINISTRATION
JACKSON AND CLAY COUNTIES, MISSOURI, AND JOHNSON
COUNTY, KANSAS**

Prospectus Number: PMO-01-LS17
Congressional District: MO 05, 06, KS 03

Certification of Need

The proposed project is the best solution to meet a validated Government need.

Submitted at Washington, DC, on August 9, 2016

Recommended: _____



Commissioner, Public Buildings Service

Approved: _____



Administrator, General Services Administration

(b) (7)(F)



**Committee on Transportation and Infrastructure
U.S. House of Representatives**

**Bill Shuster
Chairman**

Washington, DC 20515

**Peter A. DeFazio
Ranking Member**

Mathew M. Sturges, Staff Director

COMMITTEE RESOLUTION

Katherine W. Dedrick, Democratic Staff Director

**LEASE
NATIONAL INSTITUTES OF HEALTH
MONTGOMERY AND PRINCE GEORGE'S COUNTIES, MD
PMD-01-WA17**

Resolved by the Committee on Transportation and Infrastructure of the U.S. House of Representatives, that pursuant to 40 U.S.C. §3307, appropriations are authorized for a lease of up to 238,000 rentable square feet of space, including 5 official parking spaces, for the Department of Health and Human Services, National Institutes of Health currently located at 6001 and 6101 Executive Boulevard in Rockville, Maryland at a proposed total annual cost of \$8,330,000 for a lease term of up to 15 years, a prospectus for which is attached to and included in this resolution.

Approval of this prospectus constitutes authority to execute an interim lease for all tenants, if necessary, prior to the execution of the new lease.

Provided that, the Administrator of General Services and tenant agencies agree to apply an overall utilization rate of 183 square feet or less per person, except that, if the Administrator determines that the overall utilization rate cannot be achieved, the Administrator shall provide an explanatory statement to the Committee on Transportation and Infrastructure of the House of Representatives prior to exercising any lease authority provided in this resolution.

Provided that, except for interim leases as described above, the Administrator may not enter into any leases that are below prospectus level for the purposes of meeting any of the requirements, or portions thereof, included in the prospectus that would result in an overall utilization rate of 183 square feet or higher per person.

Provided that, to the maximum extent practicable, the Administrator shall include in the lease contract(s) a purchase option.

Provided further, that the Administrator shall require that the delineated area of the procurement is identical to the delineated area included in the prospectus, except that, if the Administrator determines that the delineated area of the procurement should not be identical to the delineated area included in the prospectus, the Administrator shall provide an explanatory statement to the Committee on Transportation and Infrastructure of the House of Representatives prior to exercising any lease authority provided in this resolution.

Provided further, that the General Services Administration shall not delegate to any other agency the authority granted by this resolution.

Adopted: December 7, 2016

A handwritten signature in blue ink, appearing to read "Bill Shuster", with a long, sweeping horizontal stroke extending to the right.

Bill Shuster, M.C.
Chairman

**PROSPECTUS – LEASE
NATIONAL INSTITUTES OF HEALTH
MONTGOMERY AND PRINCE GEORGE’S COUNTIES, MD**

Prospectus Number: PMD-01-WA17
Congressional District: 8

Executive Summary

The General Services Administration (GSA) proposes a lease of approximately 238,000 rentable square feet (RSF) of space for the Department of Health and Human Services - National Institutes of Health (NIH), currently located at 6001 and 6101 Executive Boulevard in Rockville, MD, under five NIH direct leases. The four leases at 6001 Executive Boulevard expire on January 31, 2019, and the one lease at 6101 Executive Boulevard expires on August 31, 2019.

The proposed lease will enable NIH to provide continued housing. The lease will significantly improve space utilization, as the office utilization rate will be reduced from 172 to 133 usable square feet (USF) per person, and the overall utilization rate from 221 to 183 USF per person, resulting in NIH being housed in approximately 31,632 RSF less space than it has at the current locations.

Description

Occupant:	National Institutes of Health
Current Rentable Square Feet (RSF):	269,632 (Current RSF/USF = 1.22)
Estimated Maximum RSF:	238,000 (Proposed RSF/USF = 1.20)
Expansion/Reduction RSF:	31,632 (Reduction)
Current Usable Square Feet/Person:	221
Estimated Usable Square Feet/Person:	183
Proposed Maximum Lease Term:	15 Years
Expiration Dates of Current Leases:	1/31/2019, 8/31/2019
Delineated Area:	Portions of Montgomery and Prince George’s Counties proximate to the NIH campus in Bethesda, MD
Number of Official Parking Spaces:	5
Scoring:	Operating lease
Estimated Proposed Rental Rate ¹ :	\$35.00 / RSF
Estimated Total Annual Cost ² :	\$8,330,000

¹ This estimate is for fiscal year 2018 and may be escalated by 1.95 percent annually to the effective date of the lease to account for inflation. The proposed rental rate is fully serviced including all operating expenses whether paid by the lessor or directly by the Government. GSA will conduct the procurement using prevailing market rental rates as a benchmark for the evaluation of competitive offers and as a basis for negotiating with offerors to ensure that lease award is made in the best interest of the Government.

**PROSPECTUS – LEASE
NATIONAL INSTITUTES OF HEALTH
MONTGOMERY AND PRINCE GEORGE’S COUNTIES, MD**

Prospectus Number: PMD-01-WA17
Congressional District: 8

Current Total Annual Cost:	\$8,314,990
----------------------------	-------------

Justification

The multiple NIH Institutes and Centers (ICs) located at 6001 and 6101 Executive Boulevard include the National Institute of Drug Abuse, National Institute of Mental Health, National Institute of Neurological Disorders and Stroke, National Institute on Deafness and other Communication Disorders, Office of Director-Office of Strategic Coordination, and the Office of Research Services, and are integral components of NIH’s mission. The current leases expire on January 31, 2019, and August 31, 2019. NIH ICs have a continuing need for space and efficient transportation access to the NIH campus in Montgomery County. The lease will streamline operations and improve NIH’s footprint by 31,632 rsf. In the absence of this reduction, the status quo cost of continued occupancy at the existing footprint would be \$9,437,120.

Acquisition Strategy

In order to maximize the flexibility in acquiring space to house the NIH elements, GSA may issue a single, multiple award solicitation in up to two proximate buildings that will allow offerors to provide blocks of space able to meet requirements in whole or in part. All offers must provide space consistent with the delineated area defined by this prospectus.

²New leases may contain an escalation clause to provide for annual changes in real estate taxes and operating costs.

**PROSPECTUS – LEASE
NATIONAL INSTITUTES OF HEALTH
MONTGOMERY AND PRINCE GEORGE’S COUNTIES, MD**

Prospectus Number: PMD-01-WA17
Congressional District: 8

Summary of Energy Compliance

GSA will incorporate energy efficiency requirements into the Request for Lease Proposals and other documents related to the procurement of space based on the approved prospectus. GSA encourages offerors to exceed minimum requirements set forth in the procurement and to achieve an Energy Star performance rating of 75 or higher.

Resolutions of Approval

Resolutions adopted by the House Committee on Transportation and Infrastructure and the Senate Committee on Environment and Public Works approving this prospectus will constitute approval to make appropriations to lease space in a facility that will yield the required rentable area.

Interim Leasing

GSA will execute such interim leasing actions as are necessary to ensure continued housing of the tenant agency prior to the effective date of the new lease. It is in the best interest of the Government to avert the financial risk of holdover tenancy.

**PROSPECTUS - LEASE
NATIONAL INSTITUTES OF HEALTH
MONTGOMERY AND PRINCE GEORGE'S COUNTIES, MD**

Prospectus Number: PMD-01-WA17
Congressional District: 8

Certification of Need

The proposed lease is the best solution to meet a validated Government need.

Submitted at Washington, DC, on August 19, 2016

Recommended: _____



Commissioner, Public Buildings Service

Approved: _____



Administrator, General Services Administration

(b) (7) (F)

Prospectus PMD-01-WA17 Map and Narrative



Within Montgomery and Prince George's counties as further delineated as follows:
Beginning at the intersection of the Potomac River and the W city boundary of Washington, DC (POB); NW along the Potomac River to Riley's Lock Road; North on Riley's Lock Road to River Road; East along River Road and continuing along Seneca Road (aka Rte 112); NE along Seneca Road to Darnestown Road (aka Rte 28); NE then SE along Darnestown Road to Muddy Branch Road; North along Muddy Branch Road to Great Seneca Highway (aka Rte 119); SE along Great Seneca Highway to Sam Eig Highway (aka I-370); NE along Sam Eig Highway and continuing E along the Intercounty Connector to Baltimore Avenue (aka Rte 1); SW along Baltimore Avenue to Powder Mill Road (Rte 212); East along Powder Mill Road to Edmonston Road (Rte 201); S along Edmonston Road, becoming Kenilworth Avenue (Rte 201) to Annapolis Road (Rte 450); W along Annapolis Road to Bladensburg Road (Alt Rte 1); W on Bladensburg Road to the E city boundary of Washington, DC; NW along the E city boundary of Washington, DC becoming Eastern Avenue NE to Western Avenue NW and the W city boundary of Washington, DC; SW along Western Avenue NW to with POB.



Committee on Transportation and Infrastructure
U.S. House of Representatives

Bill Shuster
Chairman

Washington, DC 20515

Peter A. DeFazio
Ranking Member

December 7, 2016

Mathew M. Sturges, Staff Director

Katherine W. Dedrick, Democratic Staff Director

The Honorable Denise Turner Roth
Administrator
U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405

Dear Administrator Roth:

On December 7, 2016, pursuant to section 3307 of Title 40, United States Code, the Committee on Transportation and Infrastructure met in open session to consider six resolutions included in the General Services Administration's Capital Investment and Leasing Programs.

The Committee continues to work to reduce the cost of federal property and leases. Of the six resolutions considered, the two construction projects include a federal courthouse consistent with existing funding, and the four lease prospectuses include significant reductions of leased space. In total, these resolutions represent \$56 million in avoided lease costs and offsets.

I have enclosed copies of the resolutions adopted by the Committee on Transportation and Infrastructure on December 7, 2016.

Sincerely,

Bill Shuster
Chairman

Enclosures

cc: The Honorable Peter A. DeFazio, Ranking Member